BLUETOOTH IN CORPORATE SECTOR

IMPLEMENTATION IN PAKNET

BY

MUHAMMAD ZEESHAN WAQAR (241041-009)

MUHAMMAD WAQAS (241041-001)

SUPERVISED BY

DR.IRFAN ZAFAR

A report submitted to the department of Computer Science Bahria Institute of Management and Computer Science, Islamabad for partial fulfillment of requirements for the degree of MCS

Submitted To:
Dept of computer science Bahria institute of Management and Computer Sciences (BIMCS) Islamabad.
Dept of computer Science Bahria Institute Islamabad

RESEARCHER'S DECLARATION

DATE: _____

Final Approval

We hereby solemnly declare that the work presented in this report is our own, and has not been presented previously to any other institution.

COMMITTEE:

1) SUPERVISOR

_____

2) HEAD OF DEPT

_____

3) INTERNAL

_____

4) EXTERNAL

_____

ABSTRACT

This Report is intended for the purpose of laying down the basic requirements for our project Bluetooth in co-operative sector. It defines all the functional and non-functional requirements of the system as well as its constraints. It also provides the design of the system in the form of various design documents. This report will be used as a gauging tool for our project as the project progresses.

The aim has been set quite high. It is to arrive at a specification for a technology that optimizes the usage model of all mobile computing and communications devices, and providing:

- Global usage.
- Voice and data handling.
- The ability to establish ad-hoc connections.
- The ability to withstand interference from other sources in open band.
- Very small size, in order to accommodate integration into variety of devices
- Negligible power consumption in comparison to other devices for similar use.
- An open interface standard.
- Competitively low cost of all units, as compared to their non-Bluetooth correspondents.

PROJECT BRIEF

Project Title	Bluetooth in corporate sector
Supervised By	Dr Irfan Zafer
Starting Date	May 2005
Completion Date	October 2005
Operating System	Win 98, NT, XP
System Requirements	PI or above

ACKNOWLEDGMENTS

We wish to thank all might ALLAH who has given us the chance to see and explore this beautiful world, our parents who gave us the opportunity to study in such a good institution and teachers who gave us this belief that nothing in this world is impossible and success can be achieved with hard work. This report would not have been completed without continuous support and ample guidance from our supervisor Dr. IRFAN ZAFAR

TABLE OF CONTENT

CHAPTER 1

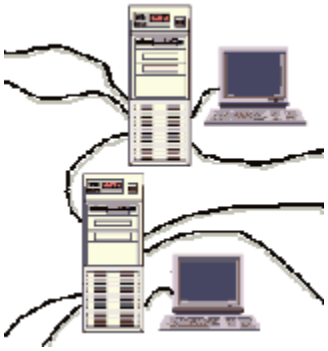
An Introduction to Bluetooth Technology

1.1 Bluetooth and why it was named Bluetooth

Bluetooth is an exciting new technology that offers wireless connectivity to an expanding array of electronic devices – computers, laptops, personal digital assistances (PDAs), cell phones, digital cameras and wireless headsets etc. Bluetooth technology enables devices to communicate seamlessly without wires. “Bluetooth is a method for data communication that uses **short-range radio links** to replace cables between computers and their connected units”. Many companies have been mulling over this idea, but it was **Ericsson Mobile Communication** that finally (in 1994) started the project. This technology was named after a tenth-century Danish King “Harald Blatand” who united Denmark and Norway. Similarly Bluetooth unites devices of different manufacturers with the help of its wireless communication link.

1.2 Why there is a wish to have a Cable Free Environment

As computerized implementations have grown and become increasingly more common in our environment, there has also been a growing need for cables of varying kinds, to tie all these units together and ensure communication between them. These cables, when they grow into a multitude, are cumbersome to handle, both directly and (even more) indirectly. Consider this list of drawbacks (below):



1. A tangle of cables.
2. Varying standards of cables and connectors.
3. Unreliable galvanic connections.
4. Need to keep cables and connectors on store.
5. Awkward to move computerized units to different locations, as cables might not be long enough.
6. Need for manual switches when the number of physical ports is not sufficient.
7. Need for re-configuration of units connection-wise in the operating system when these units are moved to a different location.

Well, then, are there no **advantages** to cabling as compared to radio waves? Yes, cabling can provide less interference from other signal sources, and they enable computers to be placed in rooms that are shielded from radio waves. But, all in all, Bluetooth is the most ambitious project we have seen this far, with the purpose of doing away with the need for cables in most instances**.**

1.3 Bluetooth´s Objectives

The aim has been set quite high. It is to arrive at a specification for a technology that optimizes the usage model of all mobile computing and communications devices, and providing:

- Global usage.
- Voice and data handling.
- The ability to establish ad-hoc connections.
- The ability to withstand interference from other sources in open band.
- Very small size, in order to accommodate integration into variety of devices
- Negligible power consumption in comparison to other devices for similar use.
- An open interface standard.
- Competitively low cost of all units, as compared to their non-Bluetooth correspondents.

1.4 Over View of IEEE 802.11 Standard

The IEEE 802.11 communications standard defines the protocol for two types of networks: **Ad-hoc and client/server**.

The **Ad-hoc** network is a simple network where communications are established between multiple stations in a given coverage area without the use of an access point or server. The 802.11- standard specifies the etiquette that each station must observe so that all units have fair access to the wireless media. It provides methods for **arbitrating** requests to use the media to ensure that throughput is maximized for all of the users in the base service set.

The **client/server** network uses an **access point** that controls the allocation of transmits time for all stations and allows mobile stations to roam from cell to cell. The access point is used to handle traffic from the mobile radio to the wired or wireless backbone of the client/server network. This arrangement allows for point coordination of all the stations in the basic service area and ensures proper handling of the data traffic. The access point routes data to and from the network server.

1.5 Bluetooth Technology- Ad-hoc Networks

The Bluetooth technology is quite complex. This is not so surprising, considering the task it has to handle. It is mainly based on the **IEEE 802.11 standard**. Of the two network modes described, Bluetooth uses the ad-hoc mode. This means that each station must observe "an etiquette" and give **all other units** fair access to the wireless media.

1.6 Features of Bluetooth Technology

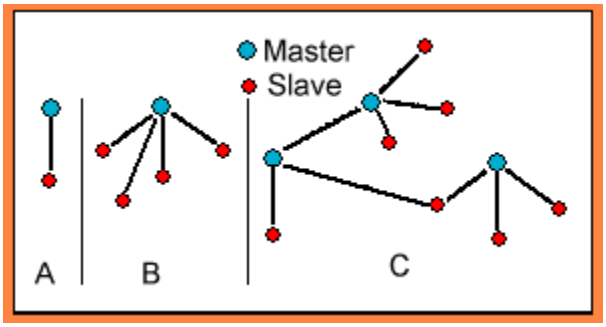
1. Bluetooth is based upon small, high performance integrated radio transceivers, each of which is allocated a unique 48-bit address derived from the IEEE 802 standards.
2. It operates in the unrestricted 2.4 GHz ISM "free band", which is available globally, although slight variation of location and width of band apply.
3. The range is set at 10 meters to optimize for target market of mobile and business user. The range can, however, be increased to 100 meters.
4. Gross data rate is 1Mbit/s, with second generation plans to increase to 2Mbit/s.
5. One-to-one connections allow maximum data transfer rate of 721 Kbits/s (corresponding to 3 voice channels).
6. Bluetooth uses a packet switching protocol, based on a frequency-hoping scheme with **1600 hops/sec.** to enable high performance in noisy radio environments. The entire available frequency spectrum is used with 79 hops of 1 MHz bandwidth, analogous to the IEEE 802.11 standard.

7. It has low power consumption, drawing only 0.3 mA in standby mode. This enables maximum performance longevity for battery-powered devices. During data transfer the maximum current drain is 30 mA. However, during pauses or at lower data rates the drain would be lower.

CHAPTER 2

BLUETOOTH DEFINITIONS

It is well to acquaint oneself with the terminology used in Bluetooth. There are 3 types of connections in Bluetooth, as shown to the right:

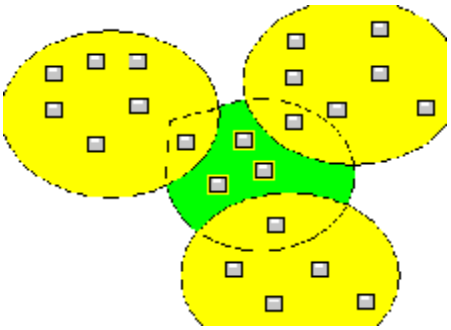


- a) Single-slave
- b) Multi-slave (up to 7 ”slaves” on one master)
- c) Scatternet

2.1 Piconet

A piconet is a collection of devices connected via Bluetooth technology in an ad-hoc fashion. A piconet starts with two connected devices, such as a portable PC and a mobile phone. The limit is set at 8 units in a piconet (that’s why the required address-space is limited to 3 bits). All Bluetooth devices are **peer units** and have identical implementations. However, when establishing a piconet, one unit will act as a master for synchronization purposes, and the other unit/units will be slave/slaves for the duration of the piconet connection.

2.2 Scatternet



A scatternet is a combination of two or more independent and non-synchronized piconets that communicate with each other. A slave as well as a master unit in one piconet can establish this connection by becoming a slave in the **other** piconet. It will then relay communications between the piconets, if the need arises.

2.3 Master unit

The device in a piconet, whose clock and hopping sequence are used to synchronize all other devices in the piconet. The master also numbers the communication channels.

2.4 Slave units

All other devices in a piconet except the master unit are called slaves (up to 7 active slave units and up to 255 parked slaves for each master can exist).

2.5 MAC address

A 3-bit Media Access Control address is used to distinguish between units participating in the piconet.

Parked Units

Parked units are the devices in a piconet which are regularly synchronized but do not have **MAC** addresses. The Master unit with the help of a “beacon signal” awakens them up. These units consume least power and are slowest with respect to the responsiveness.

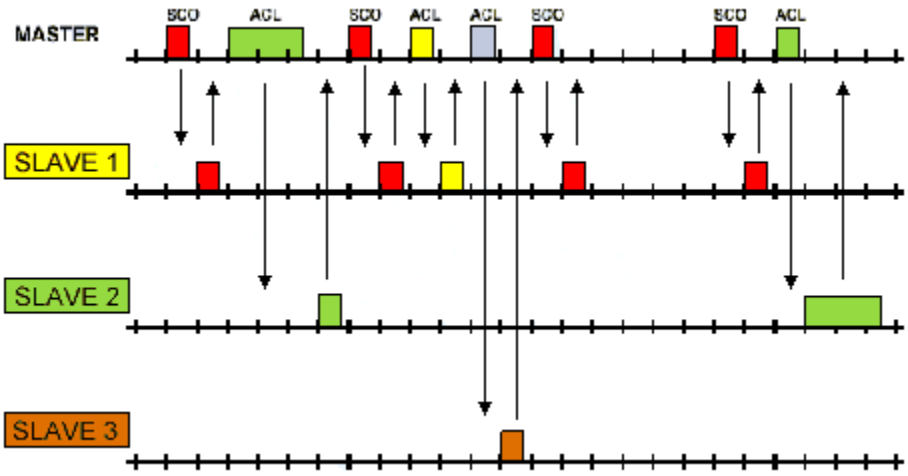
2.6 Sniff mode and hold mode

In a sniff mode, a slave becomes active periodically. In hold mode, a slave becomes idle for the entire length of the hold period. Both are power saving modes in which device activity is lowered but the slaves keep their MAC-addresses.

CHAPTER 3

BLUETOOTH PRINCIPLES

3.1 Basic Principle



Bluetooth uses **frequency hopping in timeslots.** Bluetooth has been designed to operate in noisy radio frequency environments, and uses a fast acknowledgement and a frequency-hopping scheme to make the communications link robust, communication-wise. Bluetooth radio modules avoid interference from other signals by hopping to a new frequency after transmitting or receiving a packet.

Compared with other systems operating in the same frequency band, the Bluetooth radio typically hops faster and uses shorter packets. This is because **short packages** and **fast hopping** limit the impact of microwave ovens and other sources of disturbances. Use of **Forward Error Correction** (FEC) limits the impact of random noise on long-distance links.

3.2 Two Transmission Power Levels

The Bluetooth radio is built into a small microchip and operates in a globally available frequency band ensuring communication compatibility worldwide. The Bluetooth specification has two power levels defined:

- A lower power level that covers the shorter personal area within a room
- A higher power level that can cover a medium range, such as within a home.

3.3 Communication Routes

One thing that can be noted from the figure above is that, although Bluetooth works in an ad-hoc fashion (and not server-based) all communication is done viva the **Master unit.** There is no direct communication between slave units. Nor is it intended for the Master to route messages between slave units. Rather, if slave units find that they want to talk directly to each other, they would form a new piconet, with one of them acting as Master. This does not mean that they have to **leave** the previous piconet. More likely, they will be parked in the "old" net unless they decide to quit the "old" net altogether. This is not a big decision for the slave units; reconfiguration in Bluetooth is dynamic and very fast.

3.4 Connection Establishment

In order to establish new connections the procedures **inquiry** and **paging** are used. The inquiry procedure enables a unit to discover which units are in range, and what their device addresses and clocks are. With the paging procedure, an actual connection can be established. Only the Bluetooth device address is required to set up a connection. Knowledge about the clock will accelerate the setup procedure. A unit that establishes a connection will carry out a page procedure and will automatically become the master of the connection.

For the paging process, several paging schemes can be applied. There is one mandatory paging scheme, which has to be supported by each Bluetooth device. This mandatory scheme is used when units meet for the first time, and in case the paging process directly follows the inquiry process. Two units, once connected using a mandatory paging/scanning scheme, may agree on an optional paging/scanning scheme.

After the paging procedure, the master must poll the slave by sending POLL or NULL packets, to which the slave responds. LMP procedures that do not require any interactions between the LM and the host at the paged unit’s side can then be carried out. When the paging device wishes to create a connection involving layers above LM, it sends LMP host connection req. When the other side receives this message, the host is informed about the incoming connection. The remote device can accept or reject the connection request by sending LMP accepted or LMP not accepted.

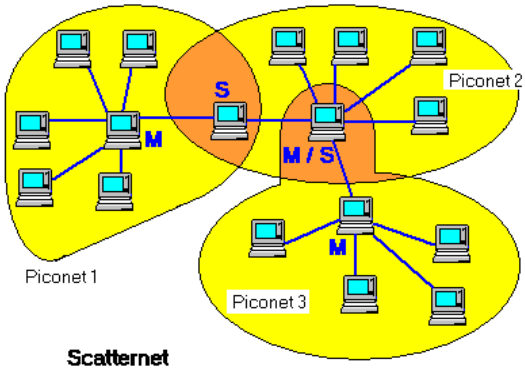
When a device does not require any further link set-up procedures, it will send LMP setup complete. The device will still respond to requests from the other device. When the other device is also ready with link set-up, it will send LMP setup complete. After this, the first packet on a logical channel different from LMP can then be transmitted.

3.5 Creating a Piconet

Piconet is a network in which up to seven Bluetooth devices can communicate with each other. A piconet can be created in one of 2 ways

- A page (used by Master to connect to Slave)
- A page scan (a unit listens for its´ device access code)

3.6 When and how is a Scatternet created?



A Master or Slave can become Slave in another piconet by being paged by the Master in this other piconet. This automatically means that any unit can create a new piconet by paging a unit that is already a member of a piconet. Any unit participating in one piconet can page the Master or Slave in another piconet. This could lead to a switch of roles between Master and Slave in this new connection.

Inter-piconet communications are established over the shared unit. Time multiplexing must be used for that unit to switch between piconets. In case of **ACL** links, a unit can request to enter the **HOLD** or **PARK** mode in the current piconet, during which time it may join another piconet by just changing the channel parameters.
Units in the **SNIFF** mode may have sufficient time to visit another piconet in between the sniff slots. If **SCO** links are established, other piconets can only be visited in the non-reserved slots in-between.

CHAPTER 4

SECURITY AND TYPE OF TRAFFIC IN BLUETOOTH

Security can mean two things in this context:

- First one is to get the surety that transmitted data must arrive in un-corrupted condition to the receiver.
- Secondly this data has not been eavesdropped by parties for whom it is not intended.

Both of these issues are (of course!) fully addressed by Bluetooth.

4.1 Safer Transmission of Data

Are the transmissions secure in a business and home environment? Yes, they are supposed to be quite reliable. Bluetooth has built in sufficient encryption and authentication and is thus very secure in any environment. In addition to this, a frequency-hopping scheme with **1600 hops/sec.** is employed. This is far quicker than any other competing system. This, together with an automatic output power adaptation to reduce the range exactly to requirement, makes the system extremely difficult to eavesdrop.

4.2 Information Integrity in Bluetooth

Information Integrity is of vital importance. We don't want the outside parties to listen in. Bluetooth has these components:

- Random Number Generation
- Encryption
- Encryption Key Management
- Authentication.

4.3 Bluetooth´s Error Correction Schemes

Bluetooth units often have to contend with electro-magnetically noisy environments. Thus, the need for some kind of error detection and correction arises. For error-detection, Bluetooth uses various checksum-calculations. When errors are detected, there are 3 error-correction schemes defined for Bluetooth:

- 1/3 rate FEC (Forward Error Correction)
- 2/3 rates FEC

- ARQ unnumbered scheme (Automatic Repeat Request).

The purpose of the **FEC** scheme on the data payload is to reduce the number of re-transmissions. However, in a reasonably error-free environment, FEC gives unnecessary overhead that reduces the throughput. Therefore, the packet definitions have been kept flexible to use FEC in the payload or not, resulting in the use of

- The **DM** and **DH** packets for the **ACL** link, and
- The **HV** packets for the **SCO** link.

The packet header is always protected by a 1/3 rate FEC; it contains valuable link information and should be able to sustain more bit errors.

4.4 Sound Transmissions

Bluetooth uses a 64 kb/s log PCM format (A-law or μ-law) or a 64 kb/s **CVSD** (Continuous Variable Slope Delta Modulation). The CVSD-format uses an adaptive delta modulation algorithm with syllabic companding. The voice coding on the line interface should have a quality equal to or better than the quality of 64 kb/s log PCM.

4.4.1 LOG PCM CODEC

Since the voice channels on the air-interface can support a 64 kb/s information stream, a 64 kb/s log PCM traffic can be used for transmission, using either A-law or μ-law compression. If the line interface uses A-law and the air interface uses μ-law or vice versa, a conversion from A-law to μ-law is performed. The compression method follows ITU-T recommendations G. 711.

4.4.2 CVSD CODEC

More robust format for voice over the air interface is a delta modulation. This modulation scheme follows the waveform where the output bits indicate whether the prediction value is smaller or larger then the input waveform. To reduce slope overload effects, syllabic companding is applied: the step size is adapted according to the average signal slope. The input to the CVSD encoder is 64 ksamples/second linear PCM.

For Bluetooth audio quality the requirements are put on the transmitter side. The 64 ksamples/s linear PCM input signal must have negligible spectral power density above 4 kHz. A set of reference input-signals are encoded by the transmitter and sent through a reference decoder (available on the website). The power spectral density, in the 4-32 kHz band of the decoded signal at the 64 ksample/s linear PCM output, should be more than 20 dB below the maximum in the 0-4 kHz range.

4.5 Fitting into the Environment

Connection speeds of up to 721 Kbps are possible, providing users with network performance that it is not much slower than a shared LAN. In theory, Bluetooth can be added to the network backbone to simplify the hot-desking. It can also allow users to synchronize address books and e-mail messages with mobile devices without having to worry about plugging in devices. But while Bluetooth will allow uses to connect to mobile devices without needing to carry external cables, current devices such as mobile phones will need adapters to work with Bluetooth.

4.6 General Features of Data Transmission

Bluetooth is specifically designed to provide low-cost, robust, efficient, high capacity, ad-hoc voice and data networking with the following characteristics:

1. 1 Mb/sec. transmission/reception rate exploits maximum available channel bandwidth.
2. Fast frequency hopping avoids interference.
3. Adaptive output power minimizes interference.
4. Short data packets maximize capacity during interference.
5. Fast acknowledge allows low coding overhead for links.
6. **CVSD** (Continuous Variable Slope Delta Modulation) voice coding enables operation at high bit-error rates.

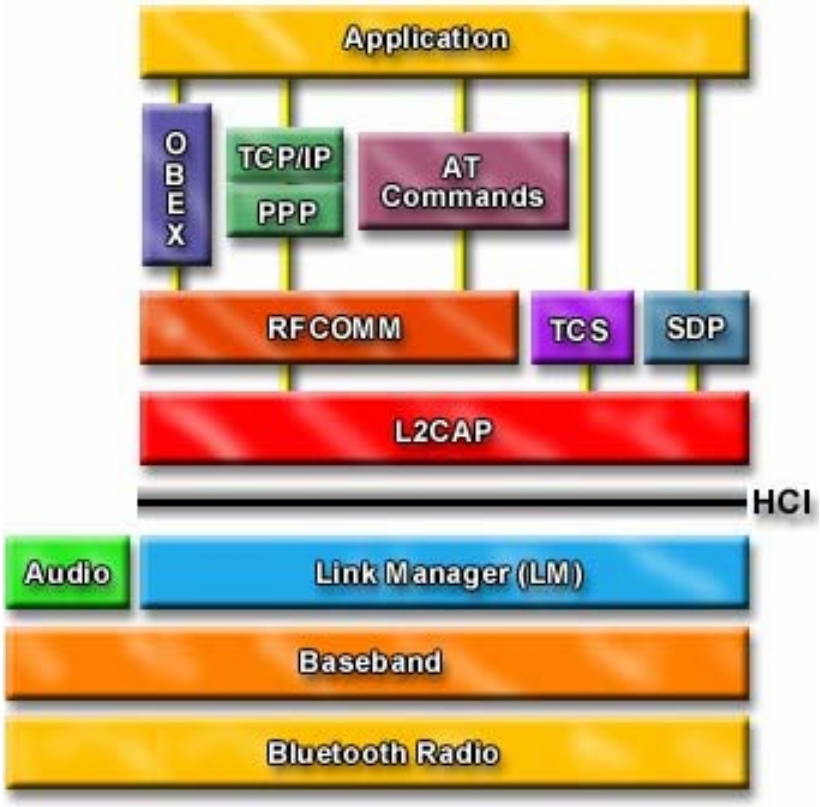
7. Flexible packet types support a wide application range.
8. Relaxed link budget supports low-cost single chip integration.
9. Transmission/reception interface tailored to minimize electric current consumption.

The Bluetooth technology was not planned to be just a physical wireless medium offering merely a platform for high-level protocols and applications. The aim is to provide something more, with immediate device-interoperability as soon as the first Bluetooth products hit the market. But this can only be achieved if all the communication blocks, including radios, protocols and applications, are accurately defined and can interoperate.

CHAPTER 5

DISCRIPTION OF LAYERS

The following is the protocol stack of Bluetooth.



A brief description of all the layers is given in this chapter.

5.1 Logical Link Control and Adaptation Protocol (L2CAP)

5.1.1 Introduction

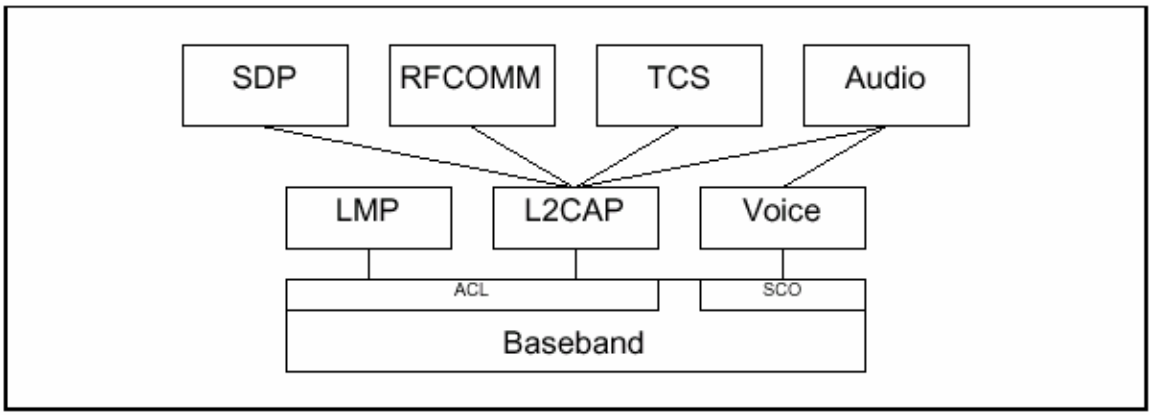
The Logical Link Control and Adaptation Layer Protocol (L2CAP) is layered over the Baseband Protocol and resides in the data link layer. L2CAP provides connection-oriented and connectionless data services to upper layer protocols with protocol multiplexing capability, segmentation and reassembly operation, and group abstractions. L2CAP permits higher-level protocols and applications to transmit and receive L2CAP data packets up to 64 kilobytes in length. Two link types are supported for the Baseband layer: Synchronous Connection-Oriented (SCO) links and Asynchronous Connection-Less (ACL) links. SCO links support real-time voice traffic using reserved bandwidth. ACL links support best effort traffic. The L2CAP Specification is defined for only ACL links and no support for SCO links is planned.

L2CAP layer is responsible for managing the logical links (connections) between the two devices. L2CAP provides connection-oriented and connectionless data services to upper layer protocols with protocol multiplexing capability, segmentation and reassembly (SAR) operation. L2CAP permits higher-level protocols and applications to transmit and receive L2CAP data packets up to 64 kilobytes in length. Since size of Baseband packet is limited (341 bytes maximum), therefore L2CAP is responsible for segmentation of larger Baseband packets into smaller size so that they can be transmitted over the hardware. Similarly at the receiving end it is responsibility of L2CAP to reassemble the packet and provide data to the upper layer. L2CAP also provides protocol-multiplexing capability, which means that many protocol layers can reside above L2CAP layer simultaneously, and L2CAP will take care of all of these layers without letting them know about existence of other layers. Each protocol layer can establish multiple logical channels with same or different Bluetooth devices.

5.1.2 L2CAP Supports Several Important Protocol Requirements

Protocol Multiplexing

L2CAP must support protocol multiplexing because the Baseband Protocol does not support any 'type' field identifying the higher layer protocol being multiplexed above it. L2CAP must be able to distinguish between upper layer protocols such as the Service Discovery Protocol, RFCOMM, and Telephony Control.



Segmentation & Reassembly

Compared to other wired physical media, the data packets defined by the Baseband Protocol are limited in size. Exporting a maximum transmission unit (MTU) associated with the largest Baseband payload (341 bytes for DH5 packets) limits the efficient use of bandwidth for higher layer protocols that are designed to use larger packets. Large L2CAP packets must be segmented into multiple smaller Baseband packets prior to their transmission over the air. Similarly, multiple received Baseband packets may be reassembled into a single larger L2CAP packet following a simple integrity check. The Segmentation and Reassembly (SAR) functionality is absolutely necessary to support protocols using packets larger than those supported by the Baseband.

Quality of Service

The L2CAP connection establishment process allows the exchange of information regarding the quality of service (QoS) expected between two Bluetooth units. Each L2CAP implementation must monitor the resources used by the protocol and ensure that QoS contracts are honored.

Groups

Many protocols include the concept of a group of addresses. The Baseband Protocol supports the concept of a piconet, a group of devices synchronously hopping together using the same clock. The L2CAP group abstraction permits implementations to efficiently map protocol groups on to piconets. Without a group abstraction, higher-level protocols would need to be exposed to the Baseband Protocol and Link Manager functionality in order to manage groups efficiently.

5.1.3 L2CAP General Operation

The L2CAP layer is based around the concept of *'channels*'. A channel identifier refers to each one of the end-points of an L2CAP channel.

Channel Identifiers

Channel identifiers (CIDs) are local names representing a logical channel end-point on the device. Implementations are free to manage the CIDs in a manner best suited for that particular implementation, with the provision that the same CID is not reused as a local L2CAP channel endpoint for multiple simultaneous L2CAP channels between a local device and some remote device.

CID	Description
0x0000	Null identifier
0x0001	Signalling channel
0x0002	Connectionless reception channel
0x0003-0x003F	Reserved
0x0040-0xFFFF	Dynamically allocated

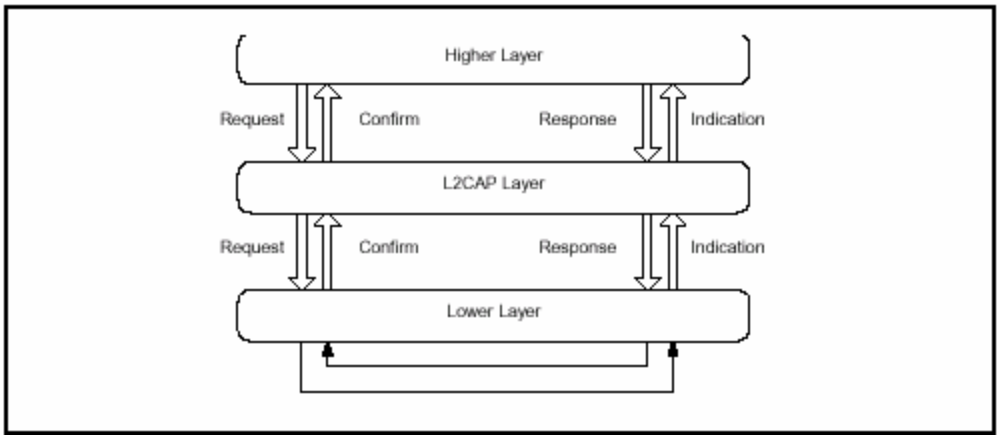
CID assignment is relative to a particular device and a device can assign CIDs independently from other devices (with the exception of certain reserved CIDs, such as the signaling channel). Thus, even if the same CID value has been assigned to (remote) channel endpoints by several remote devices connected to a single local device, the local device can still uniquely associate each remote CID with a different device.

Operation between Devices

The connection-oriented data channels represent a connection between two devices, where a CID identifies each endpoint of the channel. The connectionless channels restrict data flow to a single direction. These channels are used to support a channel 'group' where the CID on the source represents one or more remote devices. There are also a number of CIDs reserved for special purposes. The signaling channel is one example of a reserved channel. This channel is used to create and establish connection-oriented data channels and to negotiate changes in the characteristics of these channels. Support for a signaling channel within an L2CAP entity is mandatory. Another CID is reserved for all incoming connectionless data traffic.

Operation between Layers

L2CAP implementations follow the general architecture described here:



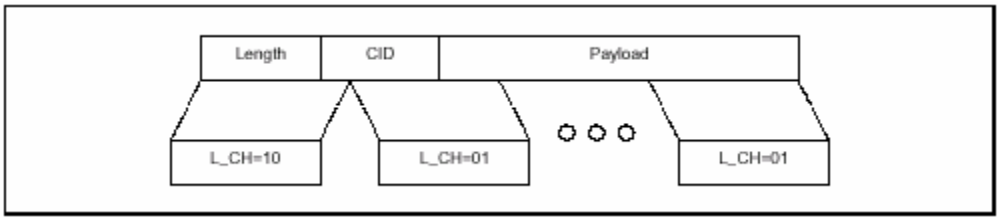
- L2CAP implementations must transfer data between higher layer protocols and the lower layer protocol.

- Each implementation must also support a set of signaling commands for use between L2CAP implementations.
- L2CAP implementations should also be prepared to accept certain types of events from lower layers and generate events to upper layers. How these events are passed between layers is an implementation-dependent process.

Segmentation & Reassembly

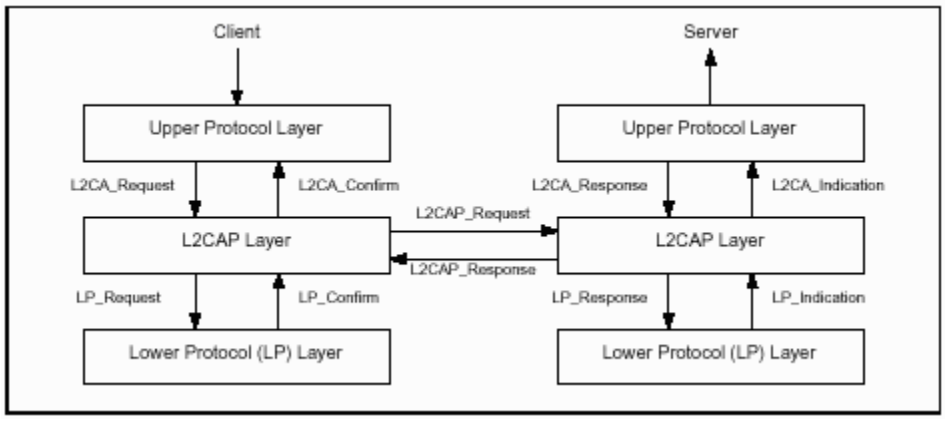
Segmentation and reassembly (SAR) operations are used to improve efficiency by supporting a maximum transmission unit (MTU) size larger than the largest Baseband packet. This reduces overhead by spreading the network and transport packets used by higher layer protocols over several Baseband packets. All L2CAP packets may be segmented for transfer over Baseband packets. The protocol does not perform any segmentation and reassembly operations but the packet format supports adaptation to smaller physical frame sizes.

An L2CAP implementation exposes the outgoing (i.e., the remote host's receiving) MTU and segments higher layer packets into '**chunks**' that can be passed to the Link Manager via the Host Controller Interface (HCI), whenever one exists. On the receiving side, an L2CAP implementation receives '**chunks**' from the HCI and reassembles those chunks into L2CAP packets using information provided through the HCI and from the packet header.



5.1.4 L2CAP State Machine

This section describes the L2CAP connection-oriented channel state machine. The section defines the states, the events causing state transitions, and the actions to be performed in response to events. This state machine is only pertinent to bi-directional CIDs and is not representative of the signaling channel or the unidirectional channel.



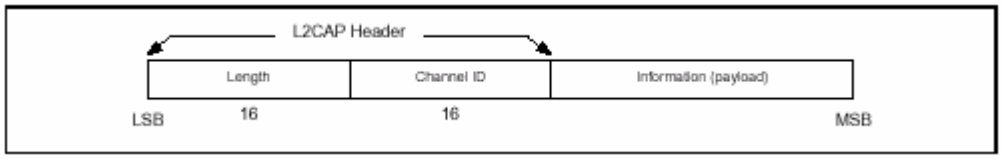
The figure above illustrates the events and actions performed by an implementation of the L2CAP layer. Client and Server simply represent the initiator of the request and the acceptor of the request respectively. An application-level Client would both initiate and accept requests. The naming convention is as follows.

- The interface between two layers (vertical interface) uses the prefix of the lower layer offering the service to the higher layer, e.g., L2CA.
- The interface between two entities of the same layer (horizontal interface) uses the prefix of the protocol (adding a P to the layer identification), e.g., L2CAP.
- Events coming from above (starting above) are called Requests (Req.) and the corresponding replies are called Confirms (Cfm).
- Events coming from below (starting below) are called Indications (Ind) and the corresponding replies are called Responses (Rsp).
- Responses requiring further processing are called Pending (Pnd). The notation for Confirms and Responses assumes positive replies. Negative replies are denoted by a ’Neg’ suffix such as L2CAP_ConnectCfmNeg.

5.1.5 Other L2CAP Features

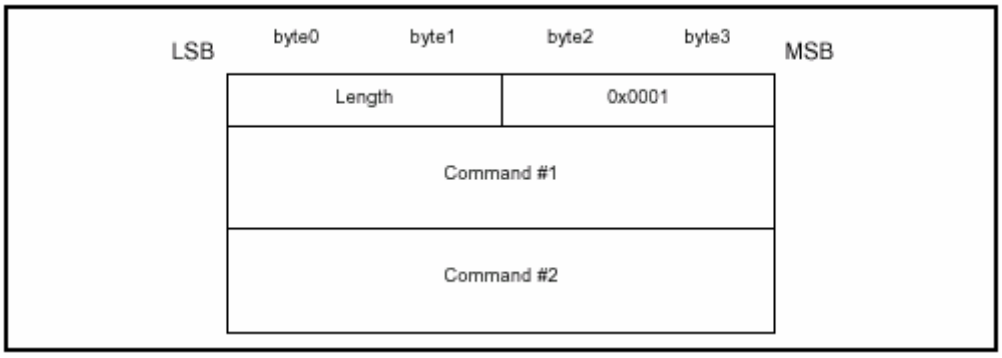
Data Packet Format

L2CAP is packet-based but follows a communication model based on *channel*s. A channel represents a data flow between L2CAP entities in remote devices. Channels may be connection-oriented or connectionless. All packet fields use Little Endian byte order.



Signaling

Various signaling commands can be passed between two L2CAP entities on remote devices. All signaling commands are sent to CID 0x0001 (the signaling channel). The L2CAP implementation must be able to determine the Bluetooth address (BD_ADDR) of the device that sent the commands. Multiple commands may be sent in a single (L2CAP) packet and packets are sent to CID 0x0001. MTU Commands take the form of Requests and Responses. For a complete list see the L2CAP specs.



Configuration Parameter Options

Options are a mechanism to extend the ability to negotiate different connection requirements. Options are transmitted in the form of information elements comprised an option type, an option length, and one or more option data fields.

Service Primitives

Several services are offered by L2CAP in terms of service primitives and parameters. The service interface is required for testing. They include primitives to:

Connection: setup, configure, disconnect

Data: read, write

Group: create, close, add member, remove member, get membership

Information: ping, get info, and request a call-back at the occurrence of an event

Connection-less Traffic: enable, disable

5.2 Host Controller Interface (HCI)

5.2.1 Introduction

The HCI provides a command interface to the Baseband controller and link manager, and access to hardware status and control registers. Essentially this interface provides a uniform method of accessing the Bluetooth Baseband capabilities**.** The HCI exists across 3 sections, the Host - Transport Layer - Host Controller. Each of the sections has a different role to play in the HCI system.

5.2.2 HCI Functional Entities

HCI Firmware (location: Host Controller)

HCI Firmware is located on the Host Controller, (e.g. the actual Bluetooth hardware device). The HCI firmware implements the HCI Commands for the Bluetooth hardware by accessing Baseband commands, link manager commands, hardware status registers, control registers, and event registers. The term Host Controller means the HCI-enabled Bluetooth device

HCI Driver (location: Host)

HCI Driver, which is located on the Host (e.g. software entity). The Host will receive asynchronous notifications of HCI events. HCI events are used for notifying the

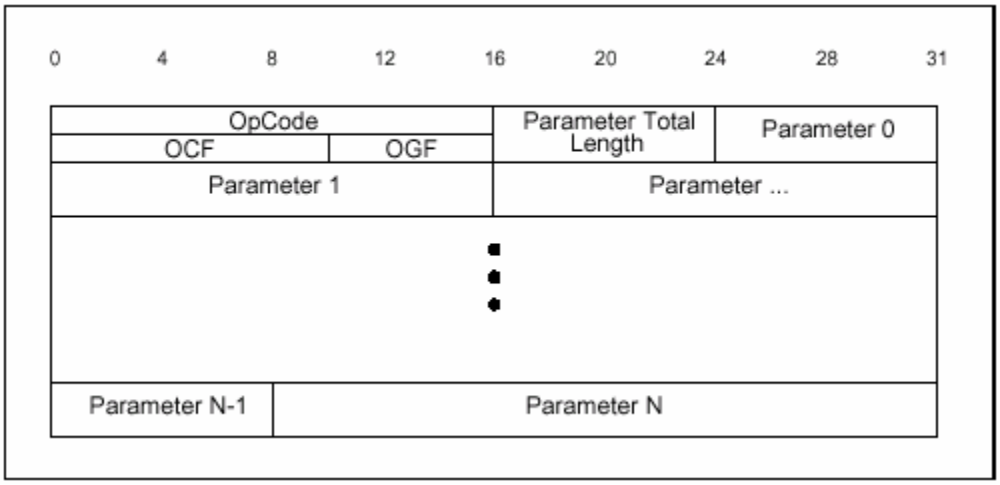
Host when something occurs. When the Host discovers that an event has occurred it will then investigate the received event packet to determine which event occurred. The term Host means the HCI-enabled Software Unit.

Host Controller Transport Layer (location: Intermediate Layers)

The HCI Driver and Firmware communicate via the Host Controller Transport Layer, i.e. a definition of the several layers that may exist between the HCI driver on the host system and the HCI firmware in the Bluetooth hardware. These intermediate layers, the Host Controller Transport Layer, should provide the ability to transfer data without intimate knowledge of the data being transferred. Several different Host Controller Layers can be used, of which 3 have been defined initially for Bluetooth: USB, UART and RS232**.** The Host should receive asynchronous notifications of HCI events independent of which Host Controller Transport Layer is used.

5.2.3 HCI Commands

The HCI provides a uniform command method of accessing the Bluetooth hardware capabilities. The HCI Link commands provide the Host with the ability to control the link layer connections to other Bluetooth devices. These commands typically involve the Link Manager (LM) to exchange LMP commands with remote Bluetooth devices. The HCI Policy commands are used to affect the behaviour of the local and remote LM. These Policy commands provide the Host with methods of influencing how the LM manages the piconet. The *Host Controller and Baseband commands*, *Informational commands*, and *Status commands* provide the Host access to various registers in the Host Controller.



HCI-Specific Information Exchange

The Host Controller Transport Layer provides transparent exchange of HCI-specific information. These transporting mechanisms provide the ability for the Host to send HCI commands, ACL data, and SCO data to the Host Controller. These transport mechanisms also provide the ability for the Host to receive HCI events, ACL data, and SCO data from the Host Controller. Since the Host Controller Transport Layer provides transparent exchange of HCI-specific information, the HCI specification specifies the format of the commands, events, and data exchange between the Host and the Host Controller.

Link Control Commands

The Link Control commands allow the Host Controller to control connections to other Bluetooth devices. When the Link Control commands are used, the Link Manager (LM) controls how the Bluetooth piconets and scatternets are established and maintained. These commands instruct the LM to create and modify link layer connections with Bluetooth remote devices, perform Inquiries of other Bluetooth devices in range, and other LMP commands.

Link Policy Commands

The Link Policy Commands provide methods for the Host to affect how the Link Manager manages the piconet. When Link Policy Commands are used, the LM still controls how Bluetooth piconets and scatternets are established and maintained,

depending on adjustable policy parameters. These policy commands modify the Link Manager behaviors that can result in changes to the link layer connections with Bluetooth remote devices.

Host Controller & Baseband Commands

The Host Controller & Baseband Commands provide access and control to various capabilities of the Bluetooth hardware. These parameters provide control of Bluetooth devices and of the capabilities of the Host Controller, Link Manager, and Baseband. The host device can use these commands to modify the behaviour of the local device.

Informational Parameters

The manufacturer of the Bluetooth hardware fixes the Informational Parameters. These parameters provide information about the Bluetooth device and the capabilities of the Host Controller, Link Manager, and Baseband. The host device cannot modify any of these parameters.

Status Parameters

The Host Controller modifies all status parameters. These parameters provide information about the current state of the Host Controller, Link Manager, and Baseband. The host device cannot modify any of these parameters other than to reset certain specific parameters.

Testing Commands

The Testing commands are used to provide the ability to test various functionalities of the Bluetooth hardware. These commands provide the ability to arrange various conditions for testing.

5.2.4 HCI Events/ Error Codes/ Flow Control

Flow Control

Flow control is used in the direction from the Host to the Host Controller to avoid filling up the Host Controller data buffers with ACL data destined for a remote device

(connection handle) that is not responding. It is the Host that manages the data buffers of the Host Controller.

HCI Events

A number of different events are defined for the HCI layer. The events provide a method to return parameters and data associated for each event. 32 HCI different events have been implemented so far, they range from *Inquiry Complete Event* to *Page Scan Repetition Mode Change Event*. See the main HCI specs for more details.

HCI Error Codes

A large number of error codes have been defined for the HCI layer. When a command fails, Error codes are returned to indicate the reason for the error. 35 HCI error codes have so far been defined, from *Unknown HCI Command* to *LMP PDU Not Allowed.* See the main HCI specs for more details.

5.2.5 Bluetooth-defined Host Controller Transport Layers

UART Transport Layer

The objective of the HCI UART Transport Layer is to make it possible to use the Bluetooth HCI over a serial interface between two UARTs on the same PCB. The HCI UART Transport Layer assumes that the UART communication is free from line errors. Event and data packets flow through this layer, but the layer does not decode them.

RS232 Transport Layer

The objective of the HCI RS232 Transport Layer is to make it possible to use the Bluetooth HCI over one physical RS232 interface between the Bluetooth Host and the Bluetooth Host Controller. Event and data packets flow through this layer, but the layer does not decode them.

USB Transport Layer

The objective of the Universal Serial Bus (USB) Transport Layer is to the use a USB hardware interface for Bluetooth hardware (which can be embodied in one of two ways: as a USB dangle, or integrated onto the motherboard of a notebook PC). A class

code will be used that is specific to all USB Bluetooth devices. This will allow the proper driver stack to load, regardless of which vendor built the device. It also allows HCI commands to be differentiated from USB commands across the control endpoint.

5.3 Bluetooth Radio

5.3.1 Introduction

The Bluetooth Radio (layer) is the lowest defined layer of the Bluetooth specification. It defines the requirements of the Bluetooth transceiver device operating in the 2.4GHz ISM band.

5.3.2 Frequency Bands and Channel Arrangement

The Bluetooth radio accomplishes spectrum spreading by frequency hopping in 79 hops displaced by 1 MHz, starting at 2.402GHz and finishing at 2.480GHz. In few countries (i.e. Spain & France) this frequency band range is (temporarily) reduced, and a 23-hop system is used in order to comply with out of band regulations in each country. In both systems a guard band is used at the lower and upper band edge.

5.3.3 Transmitter Characteristics

Power Classes

Each device is classified into 3 power classes, Power Class **1**, **2** & **3**.

Power Class 1: is designed for long-range (~100m) devices, with a max output power of 20 dBm.

Power Class 2: for ordinary range (~10m) devices, with a max output power of 4 dBm.

Power Class 3: for short-range (~10cm) devices with a max output power of 0 dBm.

The Bluetooth radio interface is based on a nominal antenna power of 0dBm. Each device can optionally vary its transmitted power.

Modulation Characteristics

The Bluetooth radio module uses GFSK (Gaussian Frequency Shift Keying) where a binary one is represented by a positive frequency deviation and a binary zero by a negative frequency deviation. BT is set to 0.5 and the modulation index must be between 0.28 and 0.35.

Spurious Emissions

The spurious emission, in-band and out-of-band, is measured with a frequency hopping transmitter hopping on a single frequency; this means that the synthesizer must change frequency between receive slot and transmit slot, but always returns to the same transmit frequency.

5.3.4 Receiver Characteristics

Sensitivity Level

The receiver must have a sensitivity level for which the bit error rate (BER) 0.1% is met. For Bluetooth this means an actual sensitivity level of -70dBm or better.

Interference Performance

The interference performance on Co-channel and adjacent 1 MHz and 2 MHz are measured with the wanted signal 10 dB over the reference sensitivity level. On all other frequencies the wanted signal should be 3 dB over the reference sensitivity level.

Out-of-Band blocking

The Out of band blocking is measured with the wanted signal 3 dB over the reference sensitivity level. The interfering signal should be a continuous wave signal. The BER should be less than or equal to 0.1%.

Maximum Usable Level

The maximum usable input level, the receiver operates at, should be better than –20 dBm. The BER should be less or equal to 0.1% at –20 dBm input power.

RSSI: Receiver Signal Strength Indicator (Optional)

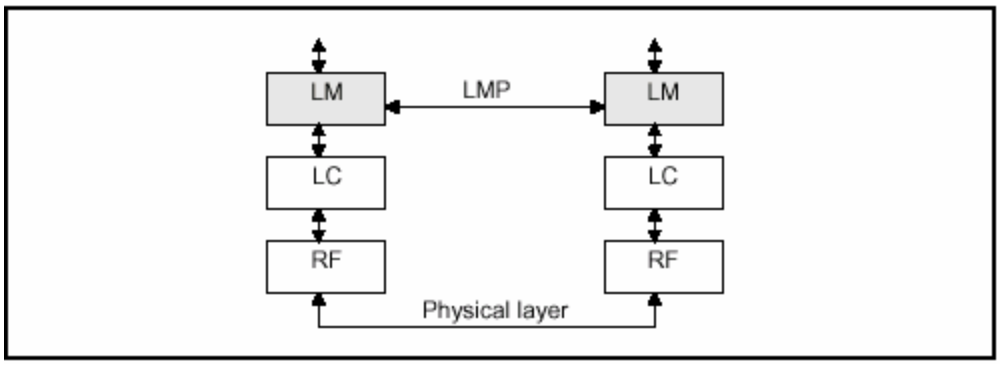
A transceiver that wishes to take part in a power-controlled link must be able to measure its own receiver signal strength and determine if the transmitter on the other side of the link should increase or decrease its output power level. A Receiver Signal Strength Indicator (RSSI) makes this possible. The way the power control is specified is to have a **golden receive power**. This golden receive power is defined as a range with a low limit and a high limit. The RSSI must have a minimum dynamic range equal to this range. The RSSI must have an absolute accuracy of ±4dB or better when the receive signal power is –60 dBm. In addition, a minimum range of 20-6 dB must be covered, starting from –60 dB and up. The instructions to alter the TX power are carried in the LMP link

5.4 Bluetooth Base band

The Base band is the physical layer of the Bluetooth. It manages physical channels and links apart from other services like error correction, data whitening, hop selection and Bluetooth security. The Baseband layer lies on top of the Bluetooth radio layer in the Bluetooth stack. The Baseband protocol is implemented as a Link Controller, which works with the link manager for carrying out link level routines like link connection and power control. The Baseband also manages asynchronous and synchronous links, handles packets and does paging and inquiry to access and inquire Bluetooth devices in the area. The Baseband transceiver applies a time-division duplex (TDD) scheme (alternate transmit and receive). Therefore apart from different hopping frequency (frequency division), the time is also slotted.

5.5 Link Manager Protocol

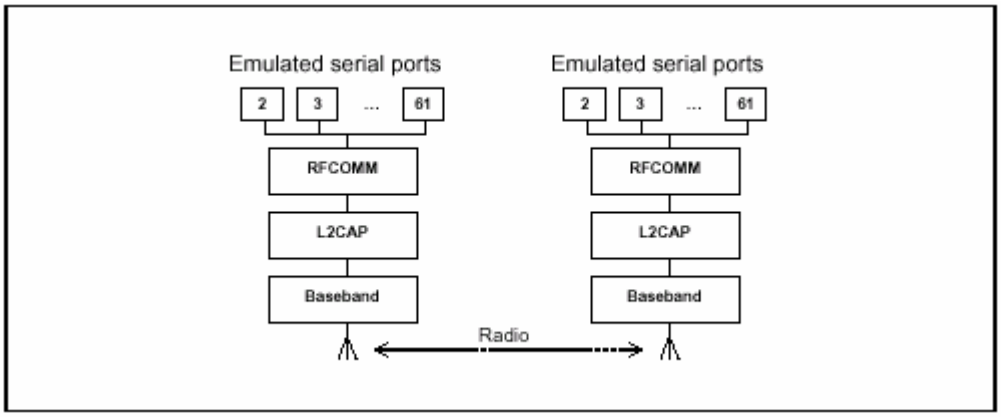
The Link Manager carries out link setup, authentication, link configuration and other protocols. It discovers other remote link managers and communicates with them via the Link Manager Protocol (LMP). To perform its service provider role, the LM uses the services of the underlying Link Controller (LC).



The Link Manager Protocol essentially consists of a number of PDU (protocol Data Units), which are sent from one device to another, determined by the AM_ADDR in the packet header. LM PDU's are always sent as single-slot packets and the payload header is therefore one byte.

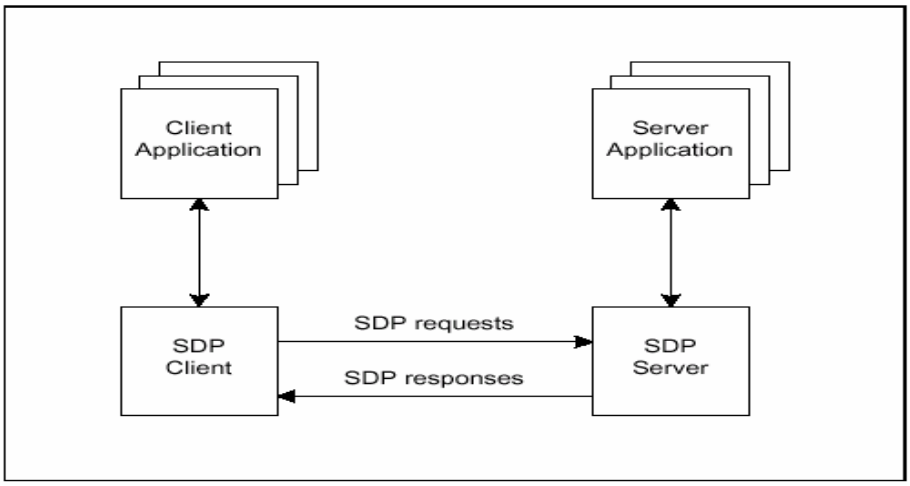
5.6 RFCOMM Protocol

The RFCOMM protocol provides emulation of serial ports over the L2CAP protocol. The protocol is based on the ETSI standard TS 07.10. Only a subset of the TS 07.10 standard is used, and some adaptations of the protocol are specified in the Bluetooth RFCOMM specification.



5.7 Service Discovery Protocol

The service discovery protocol (SDP) provides a means for applications to discover which services are available and to determine the characteristics of those available services.



A specific Service Discovery protocol is needed in the Bluetooth environment, as the set of services that are available changes dynamically based on the RF proximity of devices in motion, qualitatively different from service discovery in traditional network-based environments. The service discovery protocol defined in the Bluetooth specification is intended to address the unique characteristics of the Bluetooth environment.

CHAPTER 6

Existing Network in PAKNET

6.1 NETWORK INFRASTRUCTURE

In this chapter the existing Local Area Network in the PAKNET office is explained in detail. The network comprises of eight PC's and four Laptops which are all connected through a 24 port Cisco 2950 catalyst switch. The internet facility is provided by a radio link of 2 MB between the office and the satellite town exchange. The equipments used for the radio connectivity are a converter which converts the Ethernet data transmission to the radio waves and vice versa and a radio modem which provides the connectivity between the LAN and the radio tower. Between the switch and the radio modem there is a 2800 series router as well which provides them the platform for the internet connectivity or establishing a WAN with the outer world. To meet the requirements of printing with in the office the management has opted for a network printer instead of stand alone printers for each individual. The network printer installed is XEROX 5500. Figure 6.1 shows the complete network diagram with all the above mentioned equipment.

6.2 HARDWARE

At PAKNET the management has opted for branded systems as they provide greater reliability and more security in terms of Hardware maintenance, trouble shooting and parts assembly and replacements. The model being used is DELL OPTIPLEX GX 280 and the model for Laptop is DELL LATITUDE 600, specifications for both PC's and Laptops are given below:

6.2.1 PC Specifications

Following are the specification of PC's used at PAKNET.

Processor	Intel(R) Pentium(R) 4 CPU 3.00 GHz
Hard Disk	40 GB SATA (Maxter)
RAM	512 MB (Samsung)
VGA, Sound Card	Built IN (Realtek AC 97)
LAN Card	Realtek RTL 8139 Family PCI Fast Ethernet NIC
Mouse, Keyboard	Standard USB

6.2.2 Laptop Specifications

Following are the specifications for Laptops being used at PAKNET.

Processor	Intel(R) Centrino Pentium(R) Processor 1.60 GHz
Hard Drive	Samsung MP0402H
SD Memory	Win Bound Secure Digital Drive
RAM	1GB (Samsung)
VGA, Sound Card	Built IN (Realtek 97)
LAN Card	Realtek RTL 8139 Family PCI Fast Ethernet NIC
Wireless LAN	Intel(R) PRO/Wireless 2200 BG Network Connection
Infrared Devices	SMC IrCC – Fast Infrared Port
Bluetooth Devices	
Keyboard Mouse	Standard USB

6.2.3 Other Hardware

Network Printer	XEROX 5500
Switch/ Hub	Cisco 2950 Catalyst Switch (24 ports)
Router	Cisco 2800 series Router
Wireless Access Point	Broadcom 2.4 GHz Wireless Switch
Radio Modem	AN-30 REDLINE Radio Modem
Converter	LOOP TELECOM radio-Ethernet converter

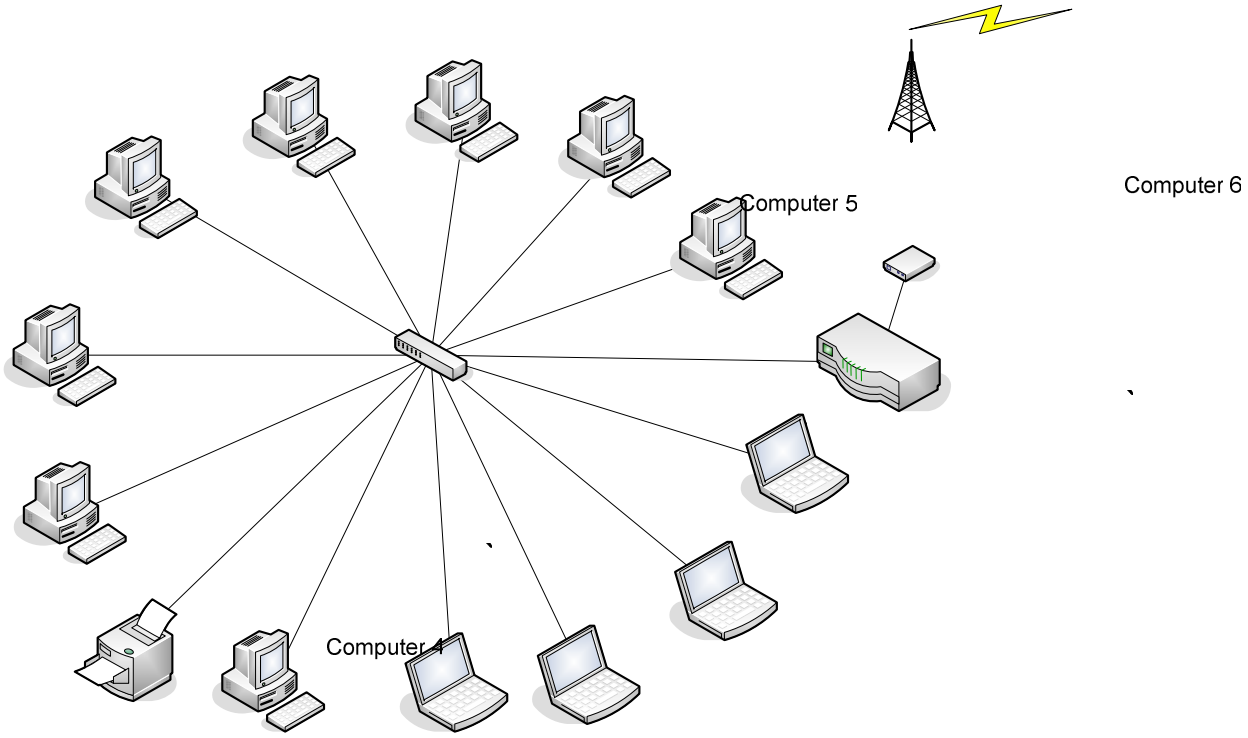
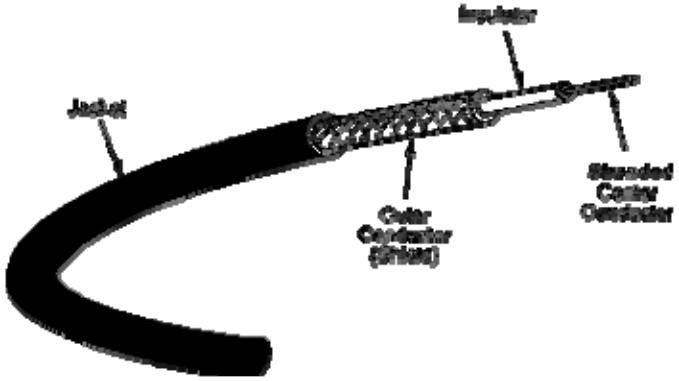


Figure 6.1: Complete network diagram at PAKNET premises.

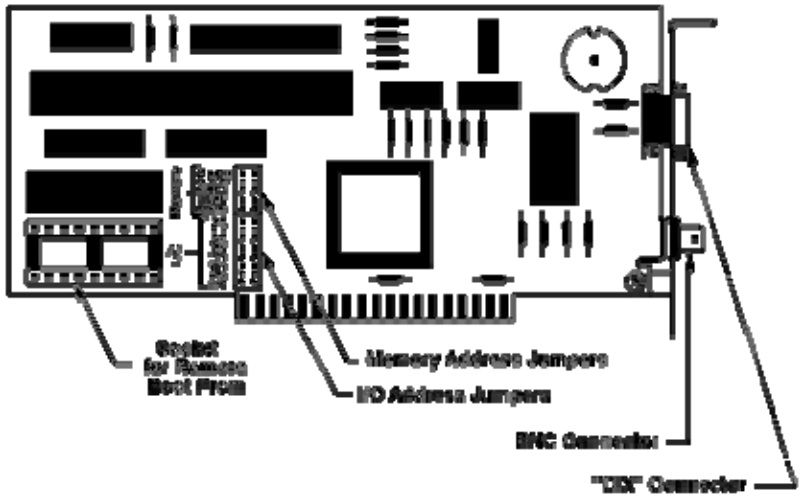
6.3 NETWORK TECHNOLOGY

Technology	:	Ethernet
Topology	:	Bus
Protocol	:	CSMA/CD
Speed	:	10Base2

Ethernet was originally developed by DIX - the Digital Corporation, the Intel Corporation, and the Xerox Corporation in the early 1970s. Ethernet is known as a spanning tree topology because the networks expand by branching in tree structures that do not allow redundant paths between nodes. Ethernet uses the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) media contention access method and supports a maximum throughput of 10 or 100 Mbps. The original Ethernet and later IEEE 802.3 protocols are similar but not usually interchangeable.



Ethernet is generally used on light to medium traffic networks, and performs best when a network's data traffic is sent in short bursts. Ethernet is the most popular network standard. It has become especially popular in many university and government installations.



6.3.1 Ethernet coax cable specifications:

RG-58 A/U, stranded conductor, CL2, 95%+ copper braided shield, PVC jacket, nominal 50 ohm impedance, 29.5 nominal capacitance/ft.

RG-58 A/U, stranded conductor, CL2P, 95%+ copper braided shield, Plenum jacket, nominal 50 ohm impedance, 27.0 nominal capacitance/ft.

RG-58/U, solid conductor, CL2, 90%+ copper braided shield, PVC jacket, nominal 50 ohm impedance. 26.0 nominal capacitance/ft.

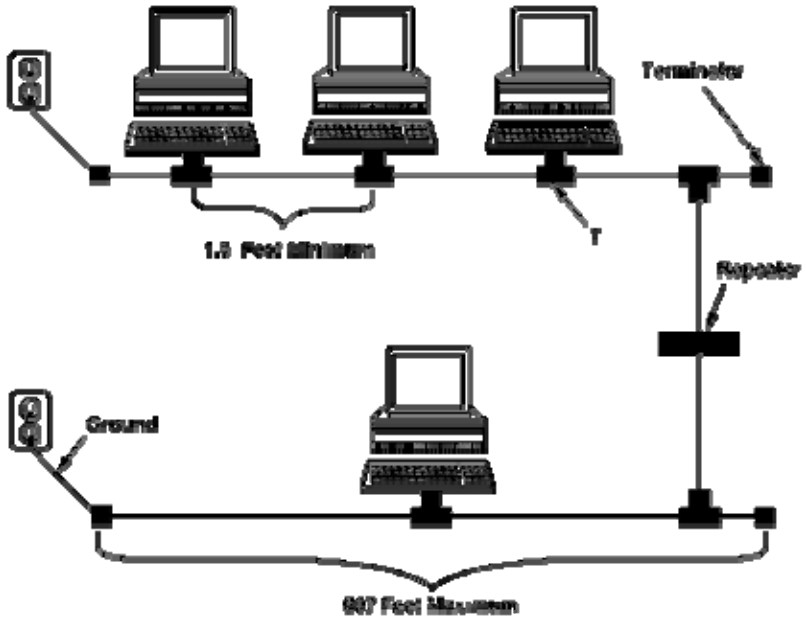
Thick Ethernet Yellow Trunk Cable, solid conductor, CL2, double foil and braided shield, PVC jacket, nominal 50 ohm impedance, 26.0 nominal capacitance /ft.

The 5-4-3 Rule

The 5-4-3 rule states that between any two nodes in the Ethernet network can be:
Up to (5) five segments in a series
Up to (4) four concentrators or repeaters
Up to (3) three populated segments (coax only)
{cable that contain nodes}

- **10Base2 (ThinNet)**

The 10Base2, thinnet topology generally uses the on-board transceiver of the network interface card to translate the signals to and from the rest of the network. Thin net cabling uses RG-58 A/U coaxial type cable, 50 Ohm terminators, and BNC T-connectors that directly attach to the connector on the NIC. A grounded terminator must be used on only one end of the network segment. The components of a thin net network are shown below.



6.4 Ethernet Protocol

A protocol is a set of rules that governs the communications between computers on a network. These rules include guidelines that regulate the following characteristics of a network: access method, allowed physical topologies, types of cabling, and speed of data transfer.

The most common protocols are:

- Ethernet
- LocalTalk
- Token Ring
- FDDI
- ATM

6.4.1 CSMA/CD Protocol is used in Paknet.

The Ethernet protocol is by far the most widely used. Ethernet uses an access method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection). This is a system where each computer listens to the cable before sending anything through the network. If the network is clear, the computer will transmit. If some other node is already transmitting on the cable, the computer will wait and try again when the line is clear. Sometimes, two computers attempt to transmit at the same instant. When this happens a collision occurs. Each computer then backs off and waits a random amount of time before attempting to retransmit. With this access method, it is normal to have collisions. However, the delay caused by collisions and retransmitting is very small and does not normally effect the speed of transmission on the network.

The Ethernet protocol allows for linear bus, star, or tree topologies. Data can be transmitted over wireless access points, twisted pair, coaxial, or fiber optic cable at a speed of 10 Mbps up to 1000 Mbps.

6.5 Ethernet Security:

When a computer is connected to the Ethernet there is the concern about the security of the data on the computer. Could the data become known by others? This is a completely

valid worry as it is relatively simple in many circumstances to see information which is passing between computers on a network. This could be exam results, references, confidential reports or passwords to other computers. What is much less likely is someone entering your computer and reading or changing data, but it is still a risk. Whilst we want to make people aware of the risks we do not want to over emphasise the problem. It would be just as easy to break into someone's car and steal their briefcase containing the same data, or see a report coming out on a communal printer. There has to be intent to compromise the privacy of the information on the Ethernet.

6.5.1 Ethernet is a broadcast system:

The primary weakness with Ethernet is that it is a broadcast system. Every message sent out by any computer on a segment of Ethernet wiring reaches all parts of that segment and potentially could be read by any computer on the segment. An analogy is shouting down a corridor "message for room five", the system operates on trust that only the person in room five will listen to the message and everyone else will ignore it. Using conventionally written software this is exactly what happens, however programs are freely available which allow all the messages on a segment to be recorded and read, or alternatively scanned for particular information.

6.5.2 Badly Configured Software:

Networks are complicated systems but offer great flexibility. You can arrange to share resources across many buildings using various network options. If however programs are not configured with thought an open door can be left for other people to access your computer. Some common examples are given below.

- **Peer-to-Peer networks:**

Peer-to-Peer networking systems such as the Macintosh AppleTalk system and Windows for Workgroups are relatively easy to install and get instant results. What can be overlooked however is that by enabling file and printer sharing you open up your files to anyone using another computer in the group. You need to carefully consider the ramifications of enabling these options.

- **FTP programs:**

An FTP program allow you to get files from and send files to another computer, which is perfectly legitimate. What is not realised however is that some FTP programs have an option in their configuration which allow other computers to FTP into your computer and have access to your files whilst the FTP program is running. The full configuration and capability of various programs need to be investigated.

- **Servers:**

Most servers (central computers) which have accounts on them are designed with a high level of intrinsic security. If however the operating system privileges are incorrectly configured users may have unintentional access to sensitive parts of the file store (its hard disks). It is up to the system administrator to ensure that there are no loopholes in the system.

- **PC-NFS:**

With NFS part of a file store on a remote computer can be made to appear as a local drive on your own computer. When reading or writing a file to the NFS drive its contents are sent down the Ethernet and can be snooped (see below). If the sharing of the file store has not been set up correctly you may unintentionally be given access to sensitive parts of the remote file store. It is again up to the system administrator to ensure that there are no loopholes in the system.

- **X-Windows:**

X-Windows is a system where a local computer can display and manipulate graphical data from a remote computer. The local and remote computer both run matched programs which exchange data between each other. Each of these programs needs to be configured only to accept connections to specific computers and to bar unknown computers from creating a connection to your machine. This is normally done by a configuration file or menu in your X-Windows program. A further risk is that unless a secure link is set up a snooper can get a display of what is on your screen.

6.5.3 Snooping the network:

The most fundamental infringement of the network is caused by someone intentionally using software which reads all the messages from the network. These programs have a

- **Printing:**

One security aspect which is often overlooked is sending a job to a printer. You may have kept all of your files secure and blocked all loopholes, only to send nearly plain text over the network to a network printer; bad news if it was an exam paper. This can be seen by a snooper exactly as if it was sent to another computer.

6.5.4 Forging:

It is relatively easy to fake an Email message which purports to come from someone else. The method used to prevent this is to use personalised encryption to ensure that the message has come from whom it says its has and can only be read by the intended person. This is briefly discussed below. It is also possible to forge a login session by recording a legitimate one and running the recording later on. Most computer systems defeat this by making the information time dependent (time stamping).

6.5.5 Catching Passwords:

Whilst not especially an Ethernet problem be aware that programs can be hidden on communal machines which sit and wait until someone goes through a logging in procedure. The password and user name are recorded and written to a hidden file for later retrieval. If a machine is not secure then obviously anyone with a blank floppy disk can steal files or leave an unwanted program on the computer.

6.6 Security Implemented at Layer 2

- **Virtual Private Networks (VPN)**

The growth of the Internet has led to many new opportunities for e-commerce and telecommuting but also considerable security challenges. Users and applications need to communicate over the Internet with the same security as if they were connected on their own private LAN. This requirement has led to development of Virtual Private Networks (VPN) as shown in Figure 1 below.

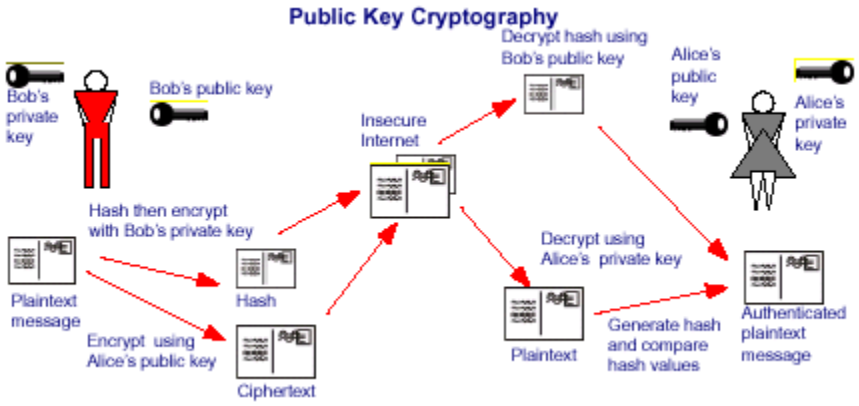
A VPN must be able to authenticate the identity of users, ensure data integrity (or recognise that it has been tampered with) and provide confidentiality by means of encryption (such that other users cannot read the data even though due to the nature of IP networks there will be many recipients of the data).

A VPN is implemented using the Internet Security Protocol (IPsec) which is an open standard extension to the TCP/IP stack specified by the Internet Engineering Task Force (ITEF) in various Requests for Comments (RFC) [Reference. 1]. IPsec specifies how cryptography is used to authenticate users, encrypt their data and guarantee data integrity. These cryptographic operations are computationally intensive but clearly the users of a VPN do not want their communications to be compromised in terms of latency or bandwidth. Therefore IPsec cryptography is ideally suited for hardware acceleration and subsequently there is a growing market of sophisticated cryptographic gateways, firewalls and network interface cards. This paper describes an Ethernet based IPsec platform targeted at that Internet security design space.

- **Public Key Cryptography**

The authentication of corresponding peers is based upon the Diffie-Hellman (DH) or Rivest-Shamir- Adleman (RSA) public key (a.k.a. asymmetric) cryptography. In these schemes every user in the network can be considered as having a private and a public key. The public and private keys are mathematically related and a message enciphered using a public key can only be deciphered using the associated private key.

The principles of public key cryptography are illustrated below.



Authentication allows Alice to be certain that Bob sent the message. To authenticate the message Bob must hash his plain text message and then encrypt this hash using his private key. Bob then sends his privately encrypted hash and publicly encrypted message to Alice.

On receipt, Alice can then decrypt the message using her private key and regenerate the message hash. She can also decrypt the encrypted hash using Bob's public key then compare the two hash values thus authenticating that Bob sent the message and confirming the integrity of the message.

Note that authentication is only performed when a session is established and hence is an infrequently executed task. However, authentication must be performed rapidly so that the user does not experience any undue latency. In fact in the BITW system described below authentication was not implemented and secure session keys were hard wired so as to minimise the software development.

- **Data Encryption Standard (DES)**

As mentioned earlier IPsec uses the Data Encryption Standard (DES) to encrypt and decrypt the actual data payload. DES is known as a symmetric algorithm because it uses the same key to encrypt and decrypt the data. That key is calculated during the authentication process.

The DES algorithm requires 16 rounds of computation to convert a plain text block of 64-bits into a cipher text block of 64-bits or vice-versa. To encrypt or decrypt a larger amount of data DES is configured to operate in a mode such as Cipher Block Chaining (CBC) where the cipher block is fed back and combined with the next input block. For

Since DES operates on the data payload it must process a maximum of 100 Mbps in each direction. Since the BITW platform requires two Ethernet ports the total data bandwidth is 400Mbps.

A typical micro-processor running at 40MHz is able to perform about 1 to 3 Mbps [Reference 3]. Motorola's recent adverts for their S1 security processors claim that a software solution would deliver 3.6Mbps. So line speed encryption is clearly a candidate for hardware acceleration.

The TDES IP used in the BITW platform is pipelined such that two rounds are performed per clock cycle and hence a single TDES operation requires 24 cycles. For 40MHz operation the maximum bit rate is therefore 106Mbps or approximately a 50X improvement over a software solution. Although not enough for the maximum theoretical bit rate it is ample for the BITW demonstration.

Similar analysis shows that SHA-1 also benefits from being implemented in hardware and the IP used achieves 252Mbps at 40MHz operation.

- **Real-Time Software**

The BITW platform and demonstration requires three software components:

1. The TCP/IP application with GUI that runs on each user PC
2. The embedded ipsec application running on the BITW platform
3. The protocol analyzer running on the snooper PC

The TCP/IP application performs two tasks; it provides the graphical user interface (GUI) for user messaging and creates a TCP/IP client-server connection between the PCs. Users can exchange text messages in clear or encrypted form and hence generate real-time data traffic on the "Internet".

The user message is entered and displayed on one PC. The message is then sent to the other PC via the two BITW platforms and received by the other PC. The original clear

The BITW application code initialises the system and performs the protocol and buffer management as frames are received and transmitted in real-time. It re-uses the MAC and IPsec C-based drivers that were available with their respective IP blocks.

The BITW application must examine and buffer each incoming packet. If it is received from the user port then it is copied across for transmission to the network port. If encryption is enabled then the packet is encrypted and a new header is created. Similarly packets received from the network port are examined and if necessary decrypted and transmitted with a new header via the user port. Hence the BITW is transparent to the two users.

The snooper can capture clear and encrypted packets but only the clear packets are human readable thus demonstrating the effectiveness of the IPsec protocol.

The snooper PC runs a public domain protocol analyser that can analyse and display all the traffic that passes through the Ethernet hub (which is representative of the entire Internet). The protocol analyzer was customised so as to capture and display the clear or encrypted frames.

The software development tools used were: the ARM Development Tools, Metrowerks Code Warrior IDE, AXD (ARM Debugger), ARM Multi-ICE and Microsoft C++.

6.7 Software

6.7.1 Operating System

Operating system acts as a driver for any computer system to work perfectly. All the systems at PAKNET come with Windows XP Professional Edition. Windows XP provides a very reliable option of firewall. Firewall stops the outside intruders and viruses to enter the system and affect its functionality. The operating system has to be reliable enough to provide security to the system as well as (in this case) the network.

6.7.2 Other Software

Antivirus

Apart from the operating systems reliability and security (Firewall) there is a need for a third party system and network security. At PAKNET the administrators are using Symantec Anti Virus. The Symantec package provides security and reliability from treats and viruses which by pass the windows security and firewall. It detects them and provides options like quarantine, delete, backup and repair. The software gives details of all the files that are deleted, quarantined and repaired. Another important feature of the software is that it maintains history of all the viruses detected, scanning of the system done from time to time and event logs are maintained for future reference purposes. There are other numerous features available in the software which provides startup scans, scheduled scans and user customized scans. Thus Symantec provides a very reliable security measure for individual systems and the network.

Printer Tracker

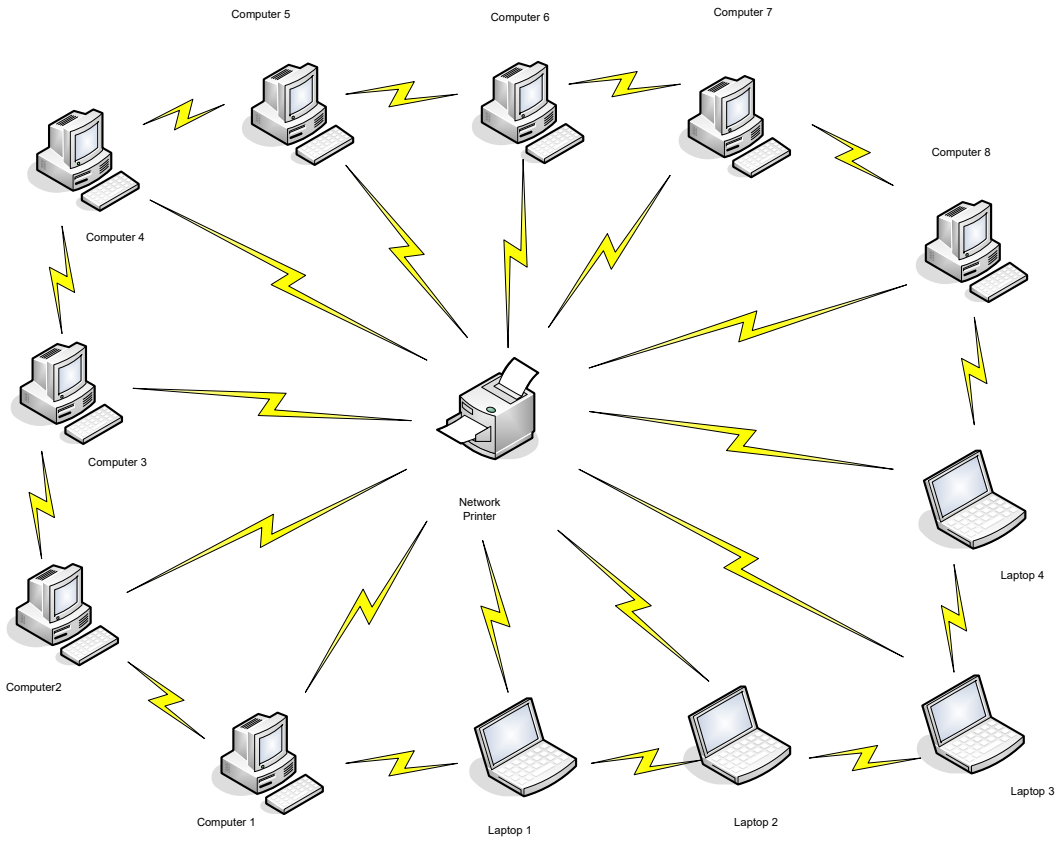
The network printer installed in the PAKNET office needs to be monitored constantly for keeping a record of the prints being taken and providing rights of printing for various users. The software used here is Print Tracker pro, this software is a great combination of administrative rights and record keeping of the print jobs. There is a need to administer the network efficiently for optimal performance that is the reason these third party software are being used to maximize the need of system and network administration.

CHAPTER 7

IMPLEMENTED (BLUETOOTH) NETWORK

In this chapter we describe in detail what our final network is, how they communicate with each other, which Bluetooth devices are used, how it is connected with WAN, and what are the software is required to communicate every device with each other.

7.1 DESIGN MODEL DIAGRAM



In the current scenario we have eight desktop Pc's four laptops and one network printer. First of all we use eight Bluetooth PCI cards in each desktop Pc's and four USB Bluetooth devices in each laptop and also use one serial to USB connector with printer and use one USB Bluetooth device with it.

Now the second step is to communicate every device with each other through some security measure.

We use software **IVT Bluesoleil 1.6** for communication among the stations with reliable security measures.

7.2 Introduction and feature of Software (IVT BlueSoleil)

BlueSoleil is Windows-based software from IVT that allows your Bluetooth enabled desktop or notebook computer to wirelessly connect to other Bluetooth enabled devices. BlueSoleil allows MS Windows users to wirelessly access a wide variety of Bluetooth enabled digital devices, such as cameras, mobile phones, headsets, printers, and GPS receivers. You can also form networks and exchange data with other Bluetooth enabled computers or PDAs.

In order to connect and share services via Bluetooth wireless technology, two devices must support the same Bluetooth Profile(s) as well as opposite device roles (i.e., one must be the server, and the other must be the client). Bluetooth enabled devices often support multiple profiles, and if involved in multiple connections, can perform different device roles simultaneously.

BlueSoleil supports the following Bluetooth functions (Profiles) in the following device roles:

Bluetooth Functions (Profiles)	Client	Server
AV Headphone*	✓	✓
Basic Image Profile	✓	✓
Dial-Up Networking	✓	
Fax	✓	
File Transfer	✓	✓
Headset*	✓	✓
Human Interface Device	✓	
LAN access	✓	✓

Object Push	✓	✓
Personal Area Networking	✓	✓
Printer	✓	
Serial Port	✓	✓
Synchronization	✓	✓

Platforms supported by BlueSoleil include:

Windows 98SE/ME

Windows 2000/XP

7.3 Mechanism being used for connection

BlueSoleil supports the following kinds of Bluetooth radio adapters: USB, CompactFlash card (UART or BCSP).

1) Insert the USB dongle to your computer.
2) Start BlueSoleil

The plug in and pull out of the USB dongle can be detected by BlueSoleil. You can start BlueSoleil first and then plug in a USB dongle.

Some Bluetooth CompactFlash cards cannot be detected when they are plugged in. Please configure the devices' parameters first.

7.3.1 Establish Bluetooth Connection

After inserting the Bluetooth card every individual station is sending a radio frequency to others the others Bluetooth stations acknowledges it and generating a connection request for a particular station that is being requested either you accept or reject its connection. If you accept its connection then a password window is appear both the stations entering the same password and making a pair with each other. Now these devices are ready for communication.

Authentication Authentication is the process of verifying "who" is at the other end of the link. Authentication is performed for devices. In Bluetooth this is achieved by the authentication procedure based on the stored link key or by pairing (entering a PIN).

Authorization Authorization is the process of deciding if device X is allowed to access service Y. This is where the concept of "trusted" exists. Trusted devices (authenticated and indicated as "trusted"), are allowed to access services. Mistrusted or unknown devices may require authorization based on user interaction before access to services is granted.

Bluetooth Connection Bluetooth functions are in the model of Client/Server. One Bluetooth device provides services, and another Bluetooth device uses these Bluetooth services. After connection, a Bluetooth link is set up between two devices, and the link is called a Bluetooth connection. Users can disconnect the connection after finishing his job on Bluetooth.

A connection is normally initiated from the client.

- On the server side, start the service.
- On the client side, initiate the connection.

7.3.1.1 Start Service on Server

If BlueSoleil provides service, please start the service:

1) Change to Service Window.
2) Right-click the service icon, select Start Service on the pop-up menu.

7.3.1.2 Initiate Connection on Client

In Main Window:

1) Single click my device, the center ball, to search the Bluetooth devices in range.

2) Search the selected Bluetooth device service by double-clicking the device icon. Service button on the top of the BlueSoleil Main Window will be highlighted if the service is supported by the device. Enter the same Bluetooth passkey on both devices if necessary to pair the two devices.
3) Connect.
   Single-click the highlighted service button to establish the connection.

7.3.2 Terminate Bluetooth Connection

After a connection is established between a client and a server, users can terminate it whenever he/she wants to. However, if the connection is terminated by force while data are being transmitted, some useful data may be lost. Please pay attention to this case.

7.4 Security of Bluetooth

To modify your connection's security settings, click My Bluetooth Security.
BlueSoleil offers three security levels:

- **Low** (Security Mode 1, No security)
  No security procedure is needed for connections.

- **Medium** (Security Mode 2, Service level enforced security)
  Authentication or Authorization is requested when a specific service is accessed by other Bluetooth enabled devices. If two devices are connecting for the first time, or if two devices do not have a trusted relationship, then the same passkey must be provided on both sides to complete the Authentication. This mode allows you to assign different access rights for each service supported by the server.

- **High** (Security Mode 3, Link level enforced security)
  If either of two devices is in Security Mode 3, Authentication is requested whenever a connection is initiated between two Bluetooth enabled devices. The passkey must be provided on both sides to complete Authentication.

7.5 Services Supported by Bluetooth

7.5.1 AV Headphone

The AV Headphone Profile enables users to use a Bluetooth enabled headphone to listen high-quality stereo music played in a computer.

Typical Usage

Listen to music using a Bluetooth enabled AV Headphone.

Steps:

1. Connect to AV Headphone.
2. Play music using media player software on your computer. Music will be transmit wirelessly to the headphone.

7.5.2 Basic Imaging

The Basic Imaging Profile (BIP) enables users to receive pictures from a Bluetooth device such as digital camera, mobile phone, or other compatible device. It also enables remote control of shooting, display, and other imaging functions.

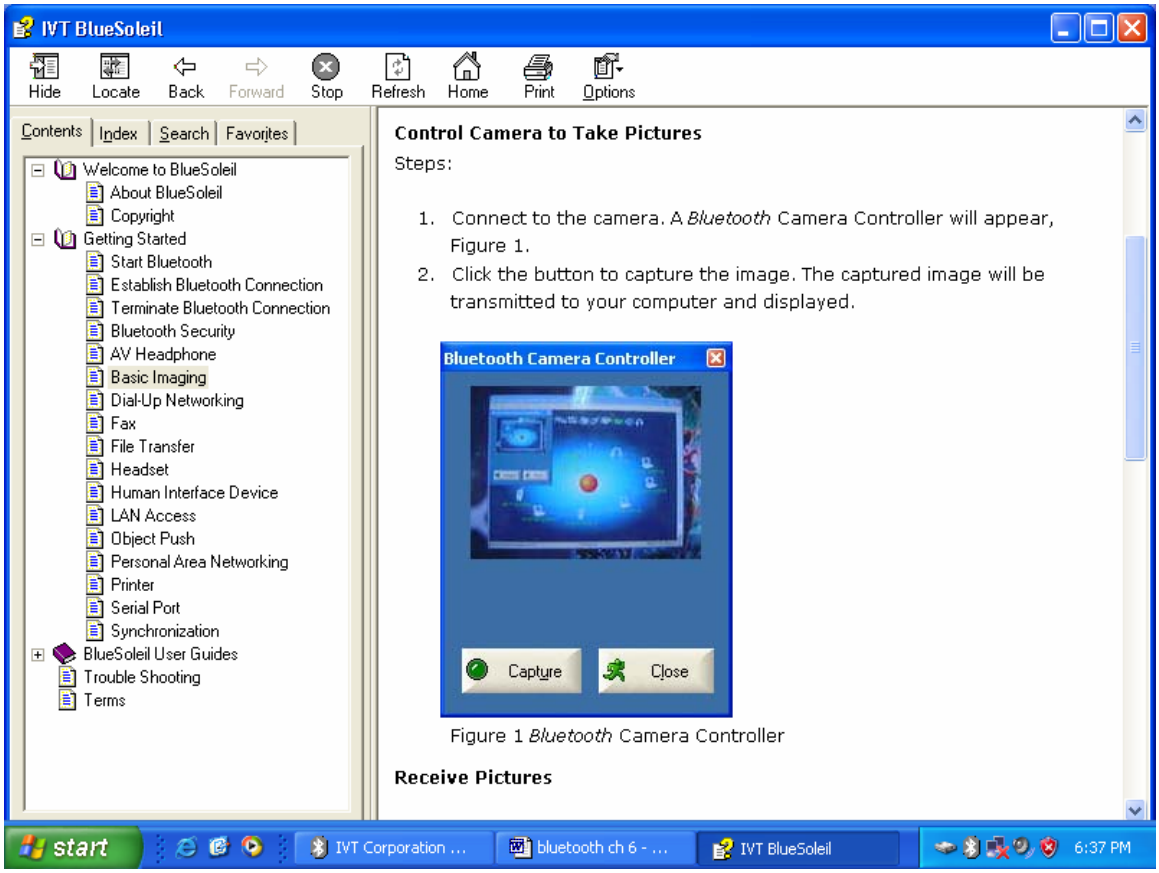
Typical Usage

- Control Camera to take pictures
- Receive pictures sent from BIP-enabled digital devices

Control Camera to Take Pictures

Steps:

1) Connect to the camera. A Bluetooth Camera Controller will appear, Figure 1.
2) Click the button to capture the image. The captured image will be transmitted to your computer and displayed.



Receive Pictures

1) Assign the directory where you would like to save image files pushed from the client device. Click My Services | Properties. Click on the Basic Image Push tab. In the Set the image directory field, browse to select the file location. Click OK.
2) Start the BIP service.
3) Send pictures from the remote device. For instructions, refer to the user documentation for the remote device.

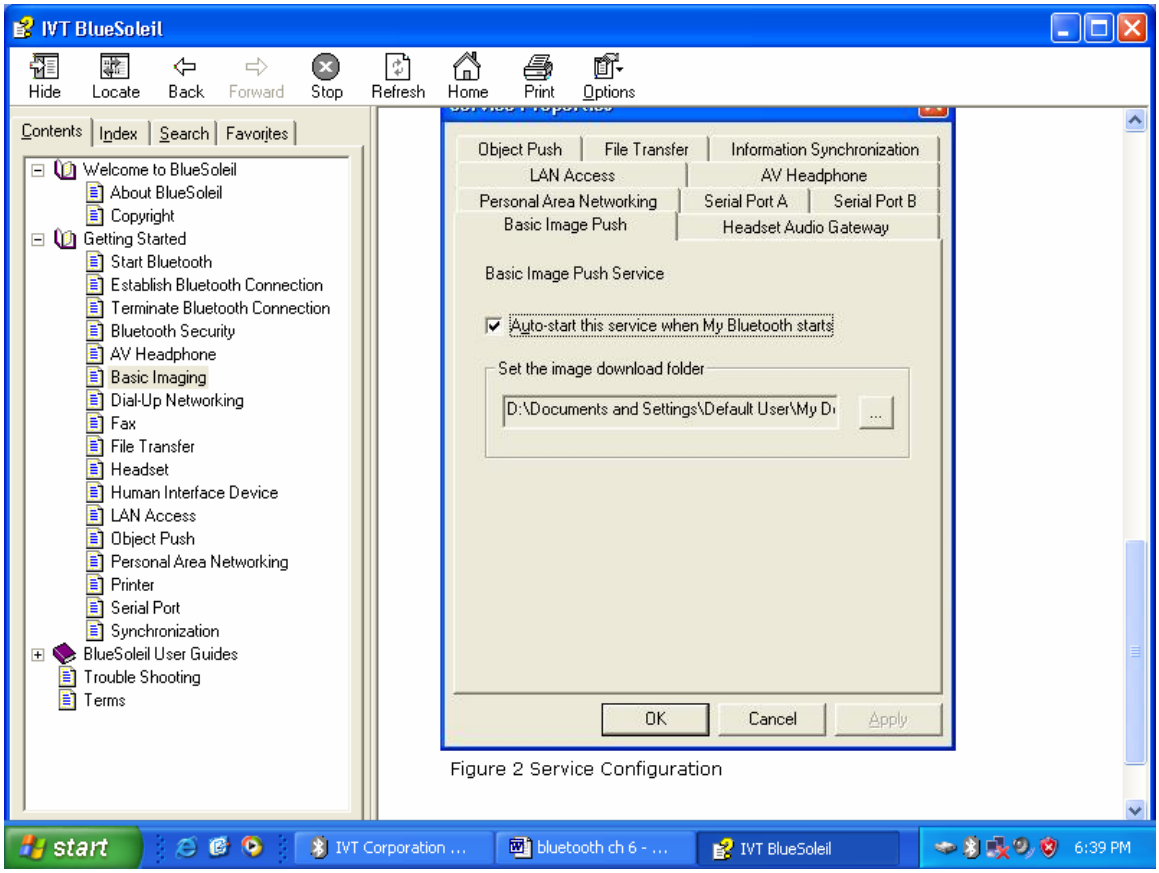


Figure 2 Service Configuration

Figure 2 Service Configuration

7.5.3 Dial-up Networking

The Bluetooth Dial-up Networking (DUN) Profile enables users to wirelessly dial-up to Internet through a Bluetooth modem or a mobile phone that supported the DUN Profile.

Typical Usage

- Dial-up to Internet via a Bluetooth enabled mobile phone.
- Dial-up to Internet via a Bluetooth enabled modem.

Dial-up to Internet via a Bluetooth mobile phone

1) Connect to the phone's Dial-Up Networking Service.
2) The Dial-Up Dialog will appear. Enter the dial-up number, User name, and Password. Make sure the correct dial-up number is entered, then click on the Dial button.

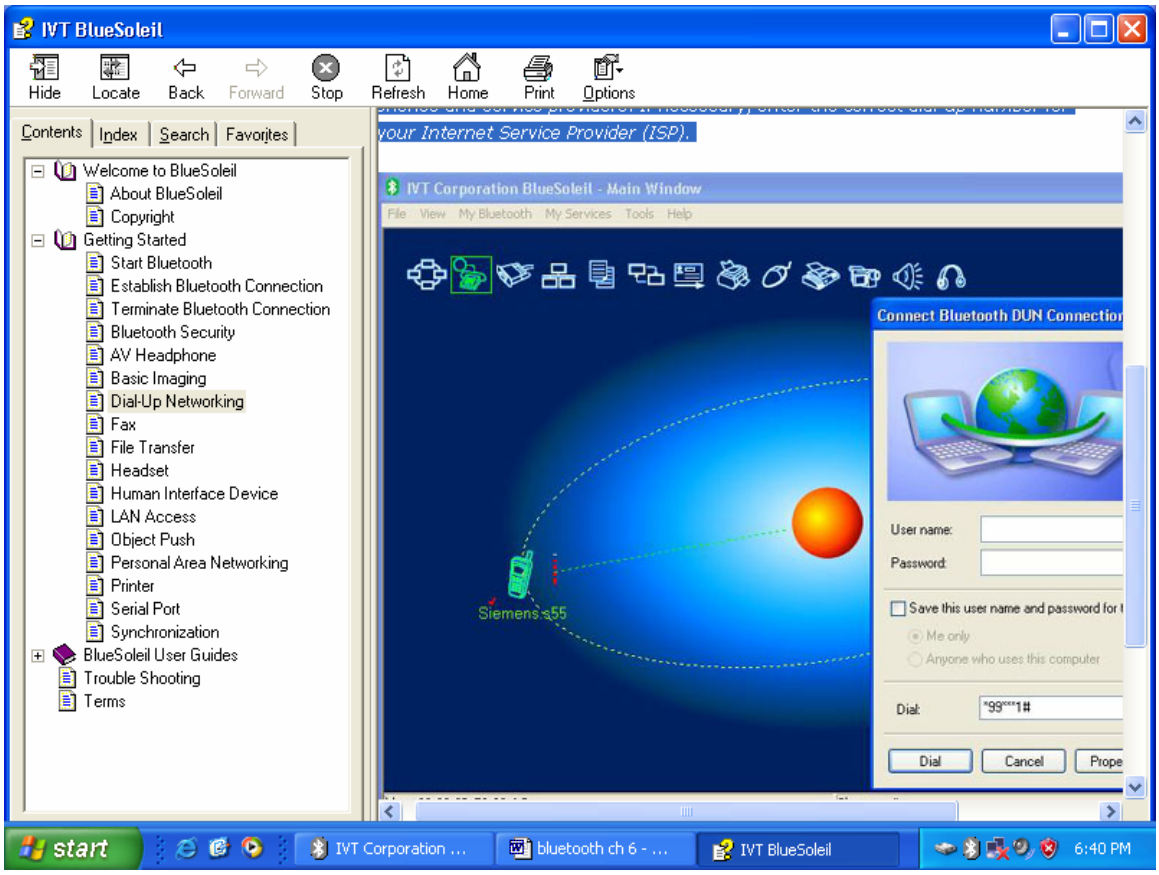


Figure 1 Dial-Up Dialog

7.5.4 FAX

The Bluetooth FAX profile enables users to send fax from a computer via a Bluetooth enabled mobile phone or modem.

Typical Usage

- Send fax via a Bluetooth enabled mobile phone.
- Send fax via a Bluetooth enabled modem.

Send Fax via Bluetooth enabled mobile phone

1) Connect to the mobile phone's FAX service.

2) Use your fax software to send the message.

Send Fax via Bluetooth enabled modem

1) Connect to the modem's fax service.
2) Start your fax software. Configure your fax software for the Bluelet Fax Modem (NOT the Bluelet Modem). Refer to your fax software's user documentation for instructions.
3) Use your fax software to send the message.

7.5.5 File Transfer

The File Transfer Profile (FTP) enables users to transfer files and/or folders between Bluetooth enabled laptops, desktops, PDAs, mobile phones, etc.

Typical Usage

- Connect to a Bluetooth enabled mobile phone and transfer files or folders to/from the phone.
- Share a folder on your computer with other Bluetooth enabled devices.
- Access a shared folder on another Bluetooth enabled device.

Connect to a Phone

Steps:

1) Connect to the phone's FTP service.
2) The phone's folders are shown in a window. Users can copy/paste/delete files or folders.

Share a Folder on Your Computer with other Bluetooth Enabled Devices

Steps:

1) Select the folder you would like to use for file sharing and define the remote user privileges. Click My Services | Properties. Click on the File Transfer tab.
   Share this folder: Browse to select the folder your would like to share.
   Share Permissions: Select Read and Write to allow others to copy, paste or delete files/folders in this folder. Select Read Only to allow others to only browse and copy files/folders from this folder.

2) Start the FTP service in BlueSoleil. Do not initiate the connection in BlueSoleil.

3) Browse your computer from the remote device. For instructions, refer to the user documentation for the remote device. When the remote device attempts to connect to your computer, the Bluetooth Service Authorization screen may appear. Click Yes.

4) After successfully connecting, the remote device can browse, copy, paste, and/or delete files on your computer, depending on the remote folder privileges you allowed. For instructions, refer to the user documentation for the remote device.

Access a Shared Folder on another Bluetooth Enabled Device

1) On the remote device, designate the folder/files to share. Enable file sharing on the remote device. For instructions, refer to the user documentation for the remote device.
   Note: If you do not enable file sharing on the remote device, BlueSoleil will not be able to discover the device's file sharing service.

2) Start the FTP service and initiate the connection in BlueSoleil.

3) A Remote Shared Folder screen will appear, displaying shared files/folders on the remote device, Use the screen to browse, copy, paste, and/or delete files, depending on your folder privileges.

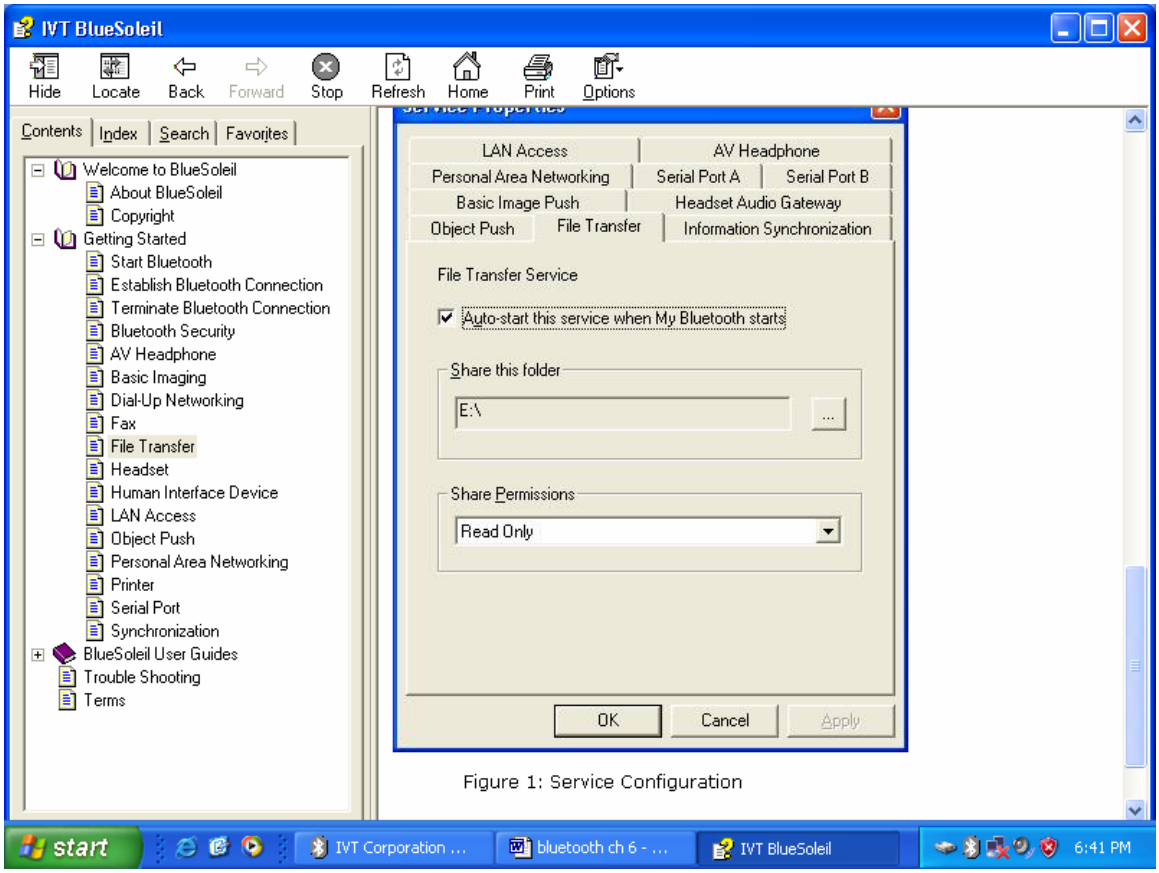


Figure 1: Service Configuration

Figure 1: Service Configuration

7.5.6 Headset

The Headset Profile enables users to use a Bluetooth headset as wireless earplug or microphone.

Typical Usage

- Use Headset as a device for audio input/output.

Use Headset as Sound Input/Output Device

Steps:

1) Connect to the Bluetooth enabled headset.

2) Play music on your computer or chat using network meeting tools. You may need to press a multifunction button on your headset to transmit audio between the computer and the headset.

7.5.7 Human Interface Device

The Bluetooth Human Interface Device (HID) profile enables users to use Bluetooth enabled HID Device such as keyboard, mice or joystick to control your computer.

Typical usage

- Connect a Bluetooth enabled Mouse and a Keyboard to Your Computer.

Connect a Bluetooth Mouse and a Keyboard to Your Computer

1) Connect the Bluetooth enabled mouse to your computer.

2) Connect the Bluetooth enabled keyboard to your computer. Before you can use BlueSoleil to connect, you may need to press a button on the keyboard to make it discoverable.

7.5.8 LAN Access

The Bluetooth LAN Access Profile (LAP) allows users to access a Local Area Network (LAN) via a Bluetooth enabled LAN access point.

Typical Usage

- Accesses a Local Area Networking via a Bluetooth enabled LAN access point.
- Use your computer as a LAN Access Point.

Access a LAN via a Bluetooth enabled Access Point (AP)

1) Connect to the LAN AP's LAP service.
2) In the Connect Bluetooth LAP Connection dialog, enter the user name and password if necessary. Click Connect.

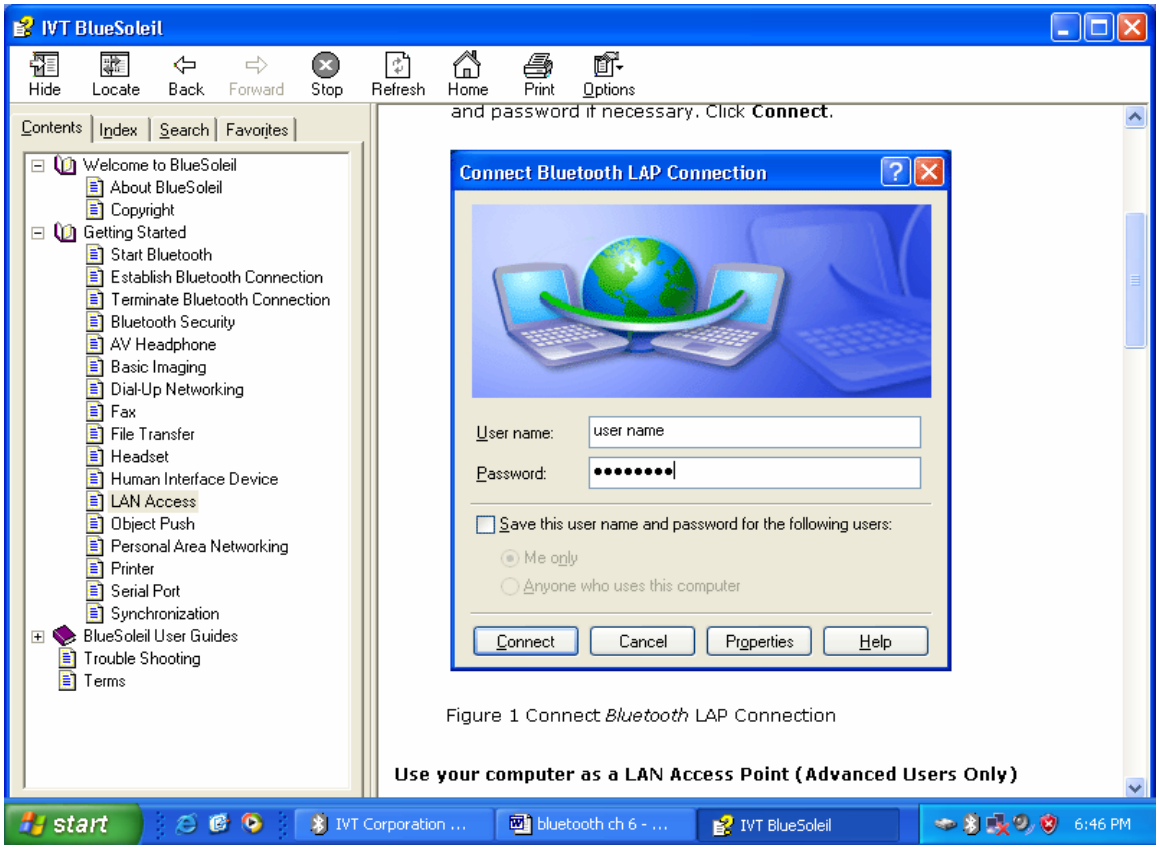


Figure 1 Connect *Bluetooth* LAP Connection

Figure 1 Connect Bluetooth LAP Connection

Use your computer as a LAN Access Point (Advanced Users Only)

1) Start the Bluetooth LAP Access service on BlueSoleil.

2) Specify any static IP addresses for LAP clients (Alternatively, you can use DHCP to have the system dynamically assign IP addresses).
(1) In the Network Connections window, right click Incoming Connection, then select Properties (Figure 2).

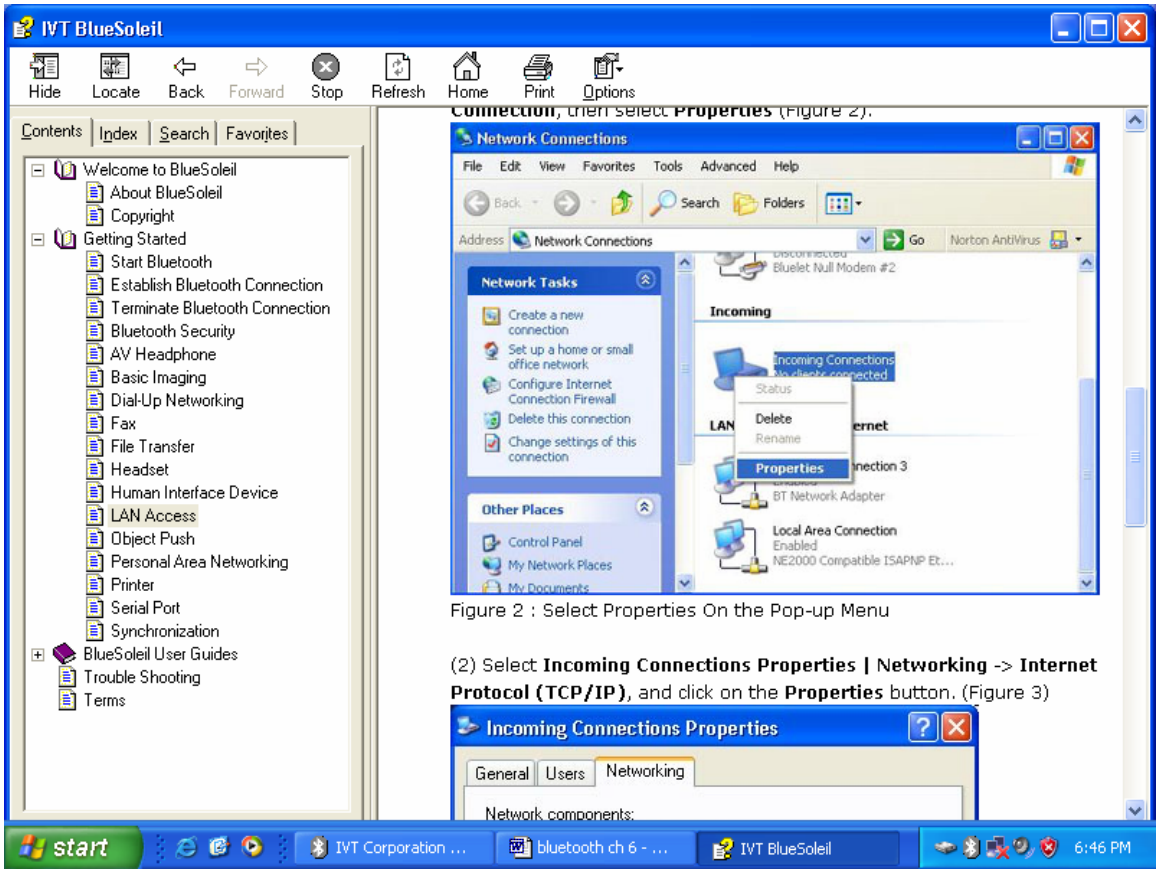


Figure 2 : Select Properties On the Pop-up Menu

(2) Select **Incoming Connections Properties | Networking -> Internet Protocol (TCP/IP)**, and click on the **Properties** button. (Figure 3)

Figure 2 : Select Properties On the Pop-up Menu

(2) Select **Incoming Connections** Properties | Networking -> Internet Protocol (TCP/IP), and click on the Properties button. (Figure 3)

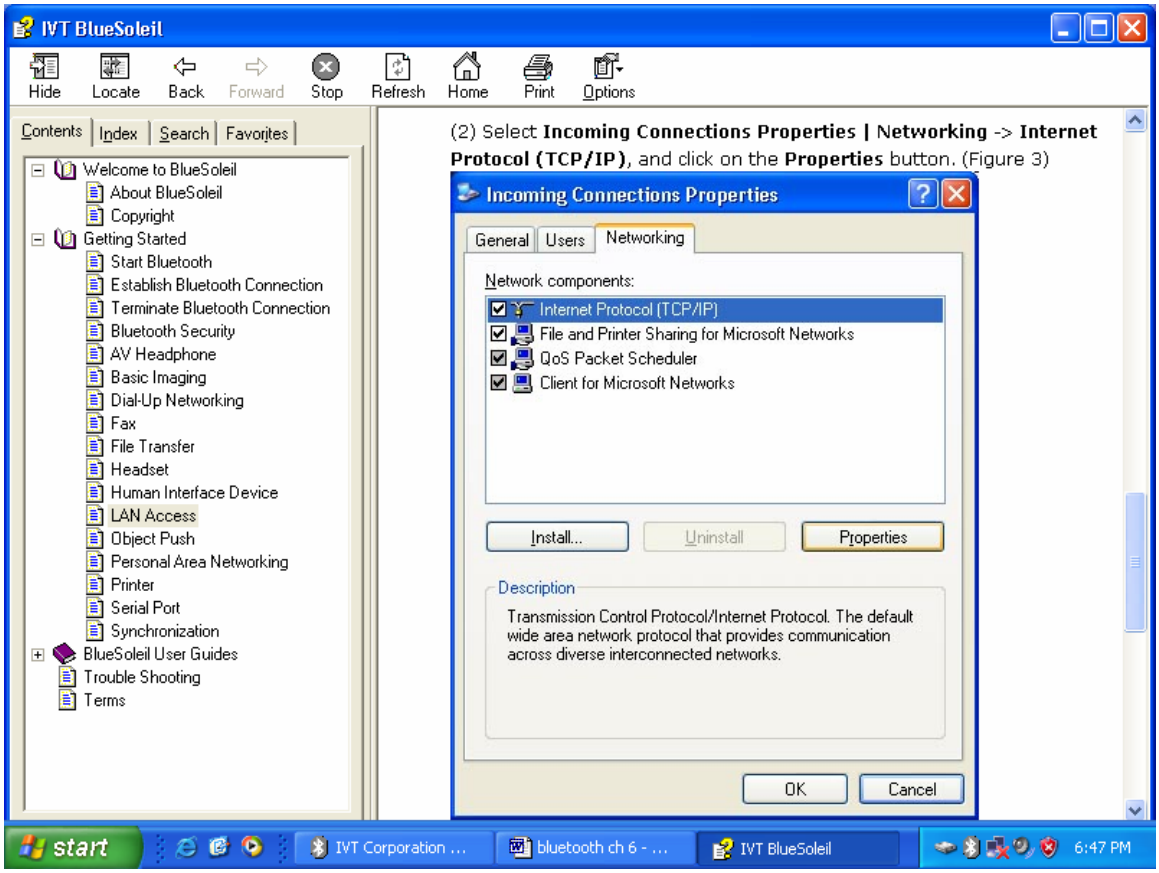


Figure 3: Internet Protocol (TCP/IP) Network Component

(3) Select **Specify TCP/IP** addresses and enter the range of IP addresses assigned to LAP clients (Figure 4).

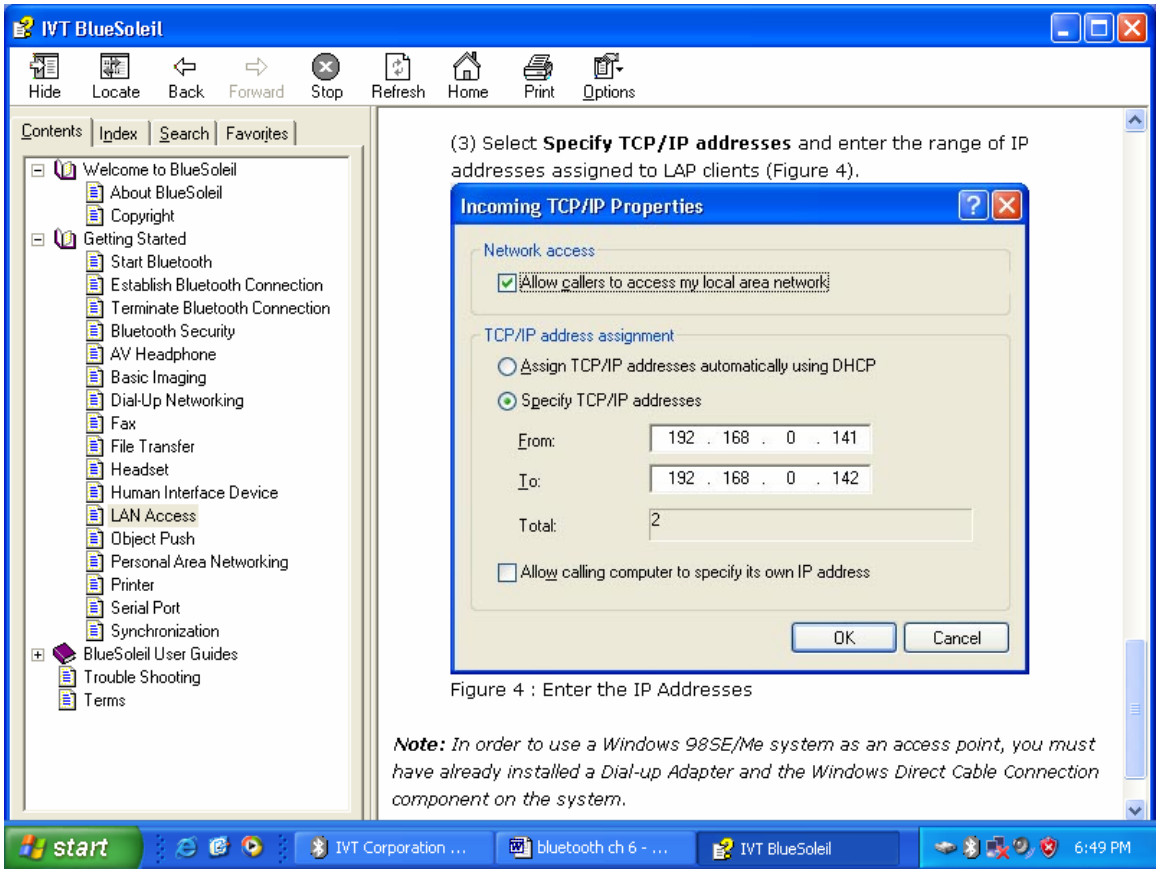


Figure 4: Enter the IP Addresses

7.5.9 Object Push

The Bluetooth Object Push profile (OPP) enables users to send and receive Personal Information Management (PIM) data objects (Including messages, notes, calendars items, and Business cards) to and from a Bluetooth enabled PDA or mobile phone.

The objects supported:

- Contacts (*.vcf)
- Calendars (*.vcs)
- Notes (*.vnt)
- Messages (*.vmg)

Typical Usage

- Push objects to a Bluetooth enabled mobile phone or PDA
- Receive objects from a Bluetooth enabled mobile phone or PDA

Push Objects to a Bluetooth Mobile Phone

There are two ways to push objects:

7.5.9.1. BlueSoleil Main Window:

Double-click on the mobile phone or PDA icon to browse for service information. The Object Push Service icon should be highlighted at the top of the screen. Right click the Object Push Service icon, and in the pop-up menu click Send My Card. (Figure 1)

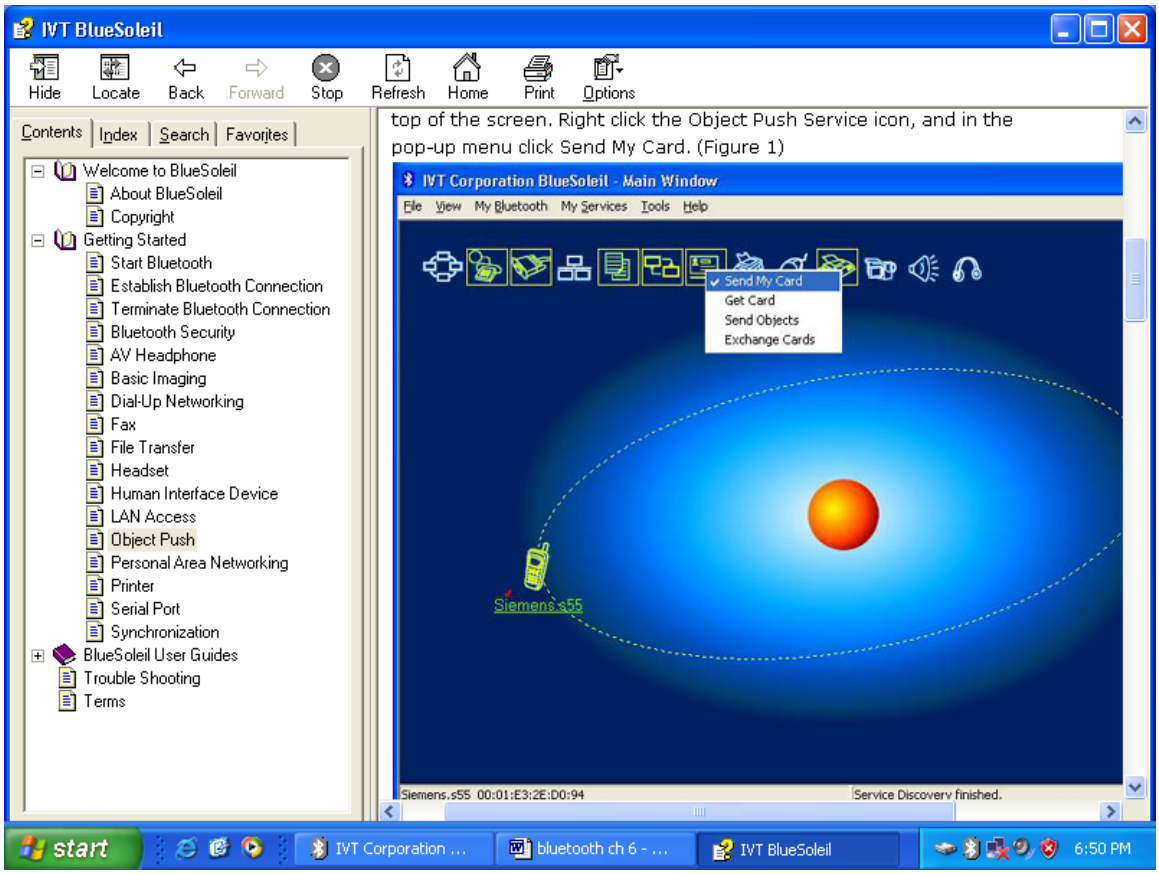


Figure 1: Send Object

- Send My Card:

  Send your default business card.

- Get Card:

  Get the default business card of the phone.
- Send Objects:

  Select some objects (PIM files in *.vcf, *.vcs, *.vnt, *.vmg) and send to phone.
- Exchange cards:

  Have your computer and the phone to exchange their default business cards.

7.5.9.2. MS Outlook:

1. Select the contact that you would like to send.
2. In Outlook, click on the Push button on the toolbar, or click File | Push.

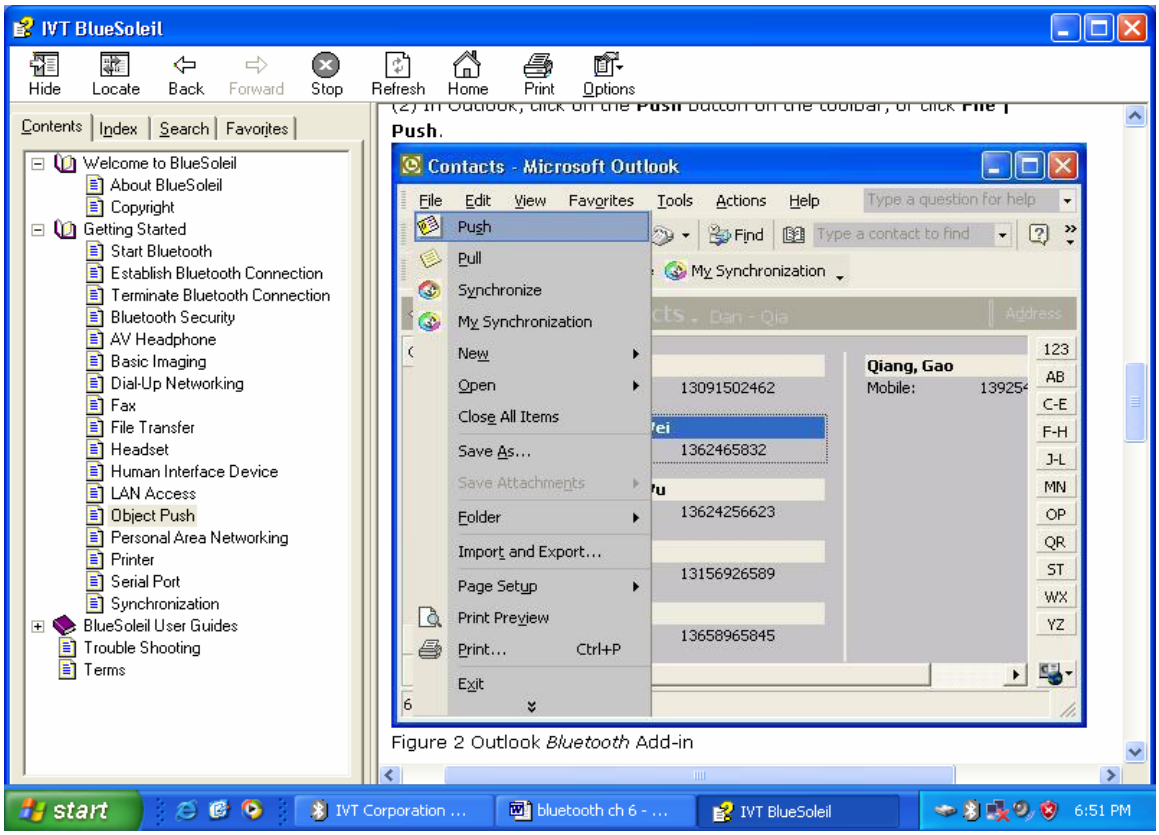


Figure 2 Outlook *Bluetooth* Add-in

Figure 2 Outlook Bluetooth Add-in

The Bluetooth Neighbors screen will appear. In the device list, select the phone or PDA that you wish to push the contact to. Click on the Push button.

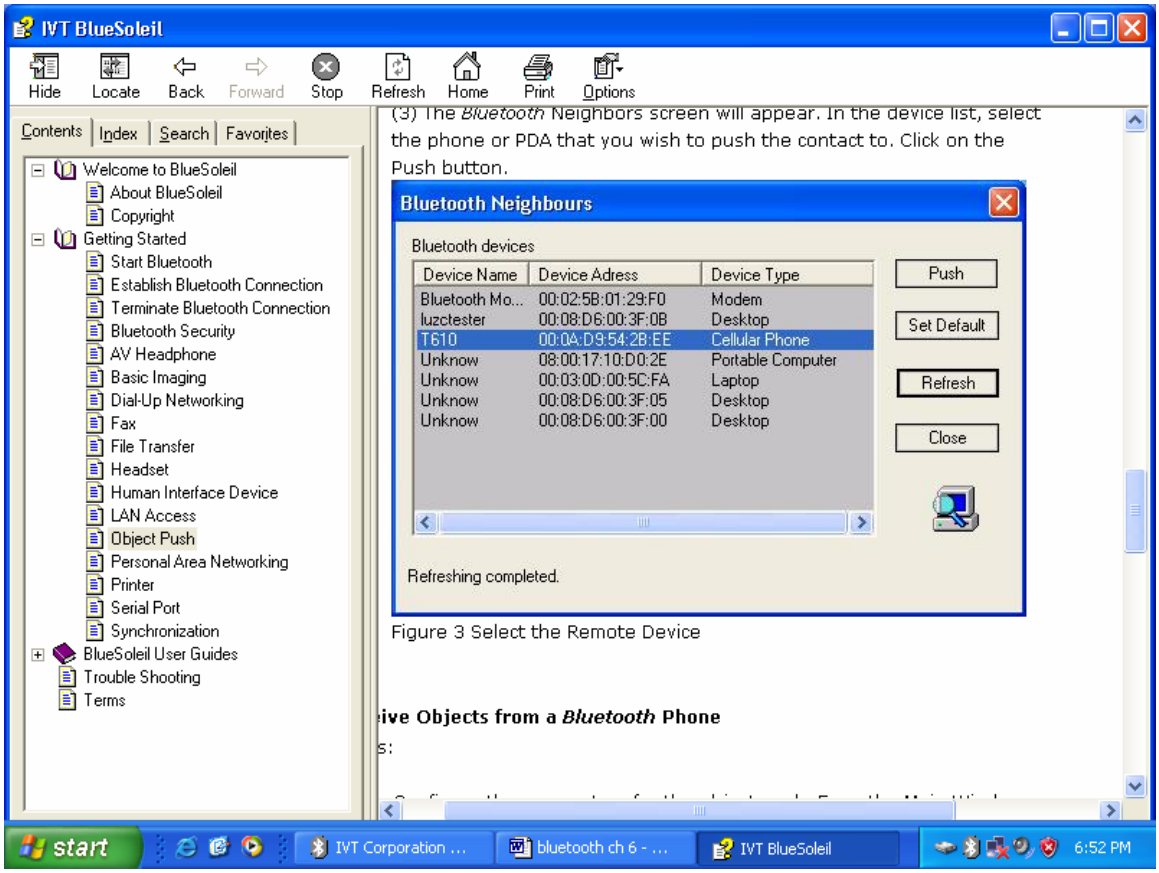


Figure 3 Select the Remote Device

Receive Objects from a Bluetooth Phone

Steps:

1. Configure the parameters for the object push. From the Main Window, click My Service | Properties. Click on the Object Push tab.

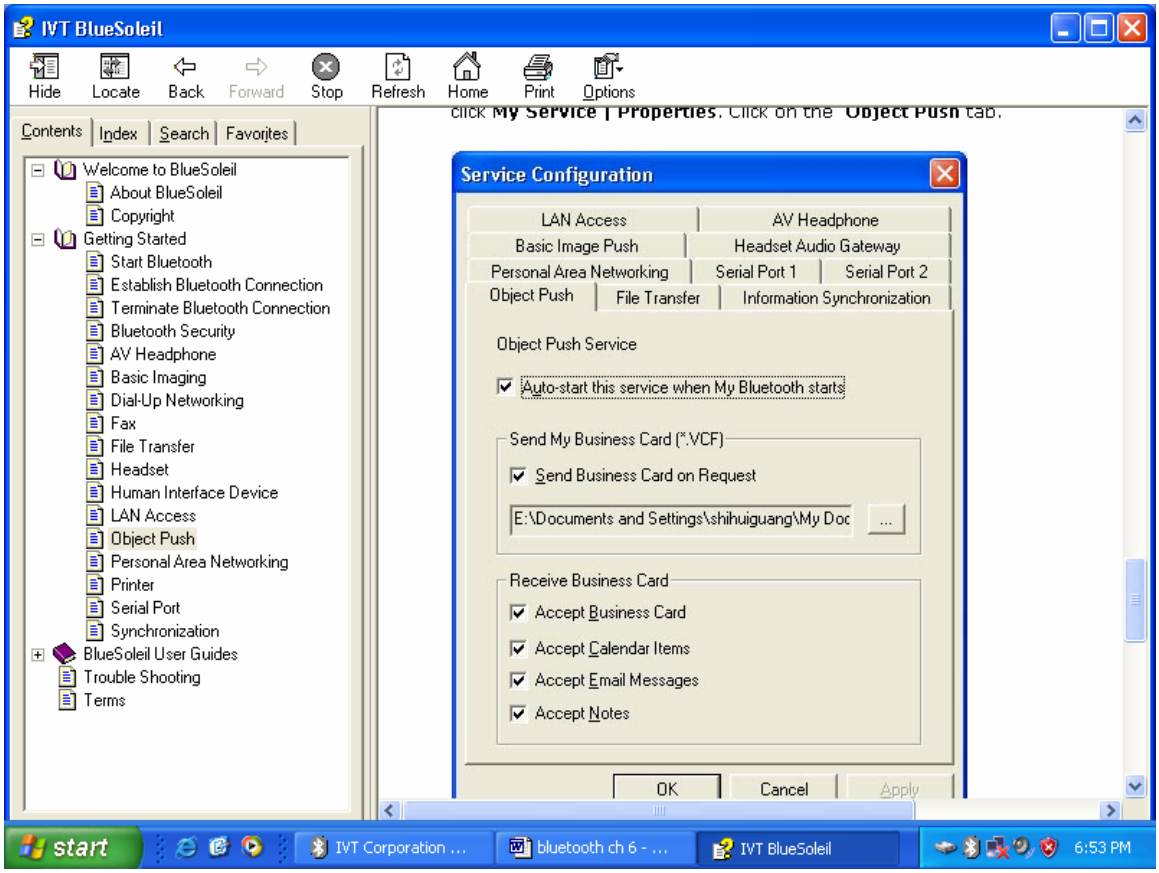


Figure 1: Object Push Service Configuration

2. Start Object Push service. Do not initiate a connection, only start the service so that your computer will be ready to receive objects.

3. Send objects from the phone. For instructions, refer to your phone's user documentation.

7.5.10 Personal Area Networking

The Bluetooth Personal Area Networking (PAN) Profile enables PCs, laptops, PDAs, and other Bluetooth enabled devices to form either of two kinds of PAN networks. In a Group ad-hoc Network (GN), which functions as an isolated network, multiple PAN Users (PANUs) are linked together via a GN controller. Alternatively, a PAN can consist of multiple PANUs linked to a Network Access Point (NAP), which provides access to external Local Area Network (LAN) infrastructure. BlueSoleil supports all three of these device roles — GN (controller), PANU, and NAP.

Typical Usage

- Group Ad-hoc Network (Peer-to- peer networking)
  One device acts as the GN, and others function as PANU devices. These computers can visit each other or use an application based on TCP/IP.

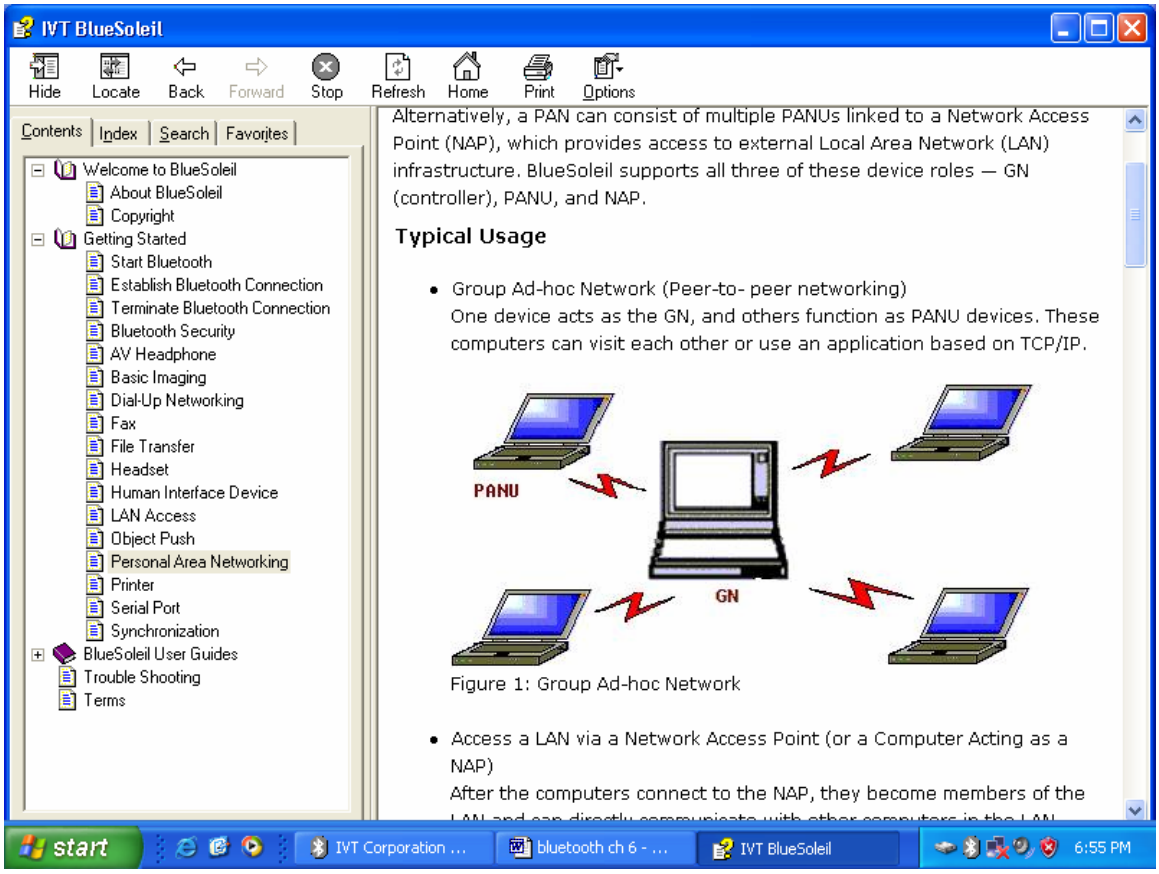


Figure 1: Group Ad-hoc Network

- Access a LAN via a Network Access Point (or a Computer Acting as a NAP)
  After the computers connect to the NAP, they become members of the LAN and can directly communicate with other computers in the LAN.

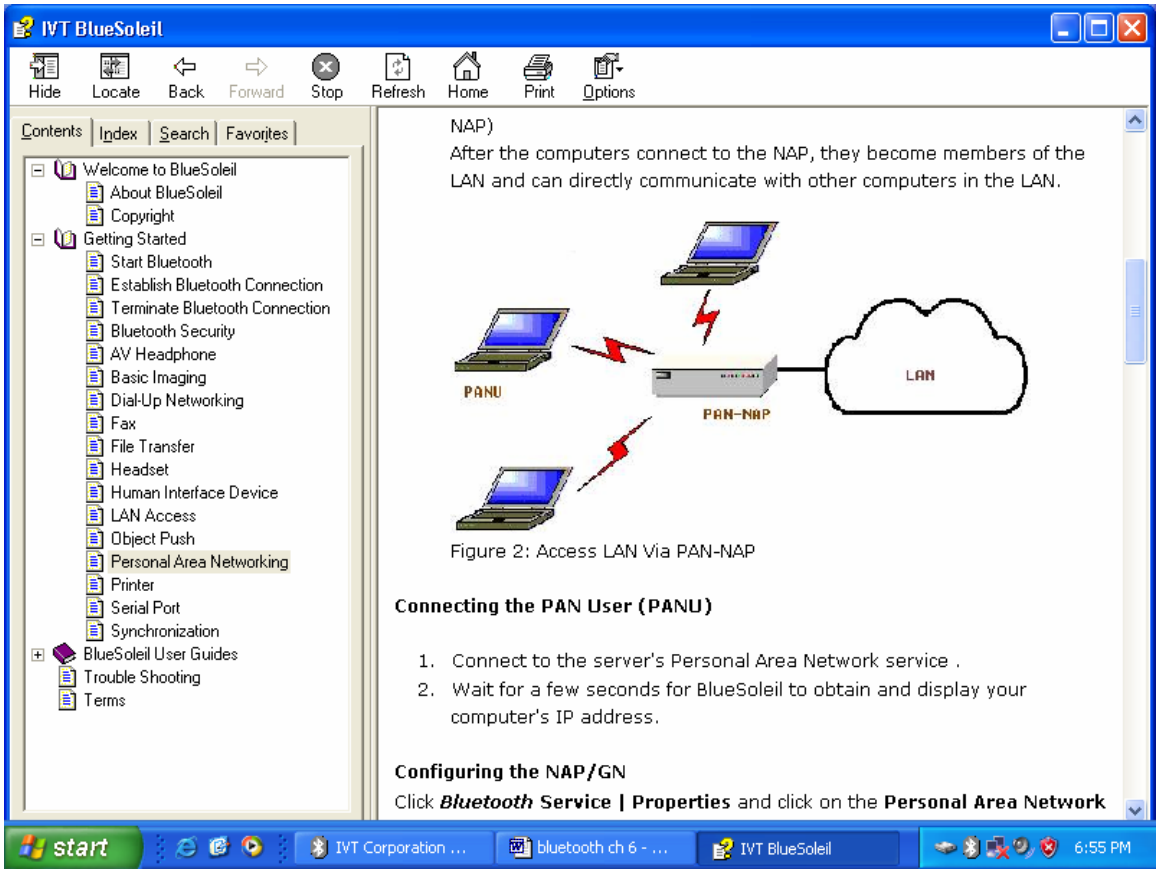


Figure 2: Access LAN Via PAN-NAP

7.5.10.1 Connecting the PAN User (PANU)

1. Connect to the server's Personal Area Network service.
2. Wait for a few seconds for BlueSoleil to obtain and display your computer's IP address.

7.5.10.2 Configuring the NAP/GN

Click Bluetooth Service | Properties and click on the Personal Area Network tab.

- **Scenario 1**: Group Ad-hoc Network

  Select Set up Bluetooth Personal Area Network and Enable DHCP Server (Figure 3).

  A DHCP server will be started on the GN. The PANU can obtain an IP address

automatically from this DHCP server if the PANU does not set static IP address for the **BT Network Adapter.**

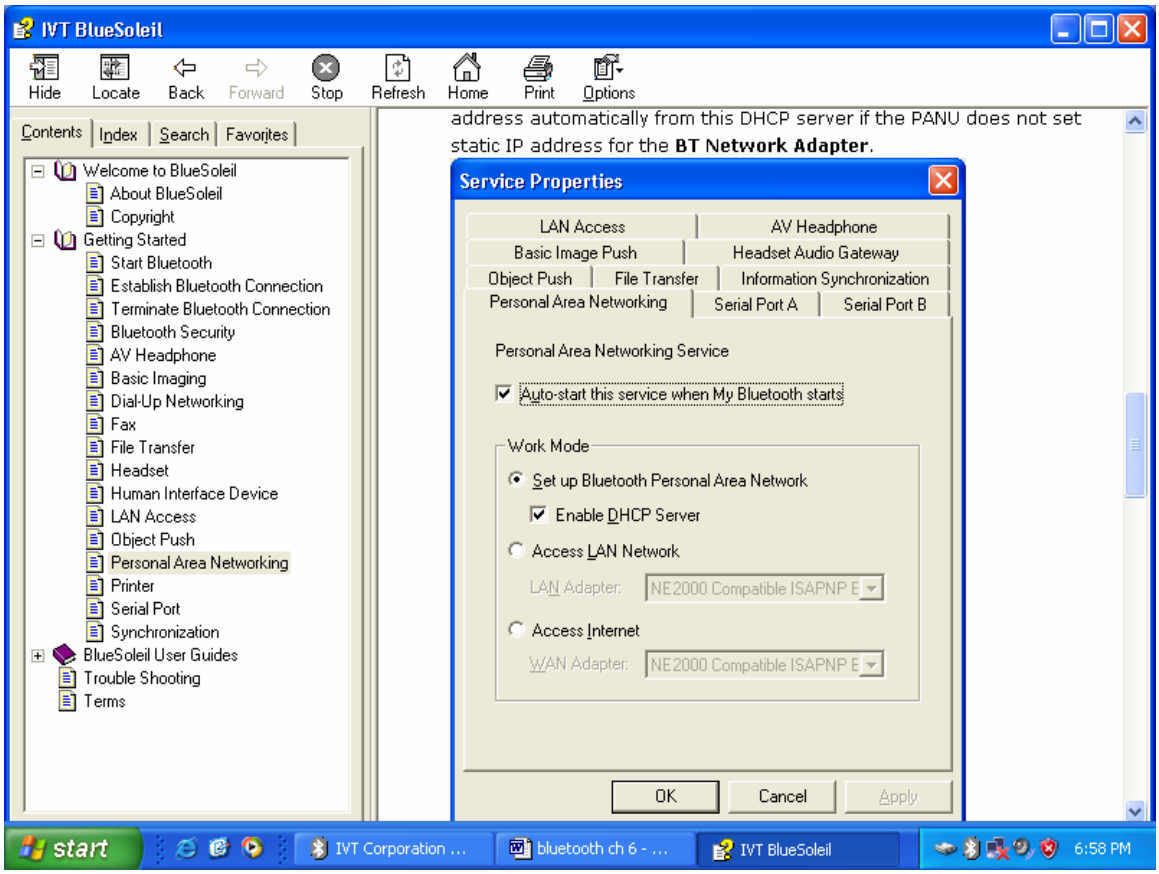


Figure 3: Set Up Bluetooth Personal Area Network

- **Scenario 2**: Access LAN via PAN-NAP

  Select Access LAN Network and select a physical network adapter, through which the NAP connects to a LAN, as the LAN Adapter (Figure 4).

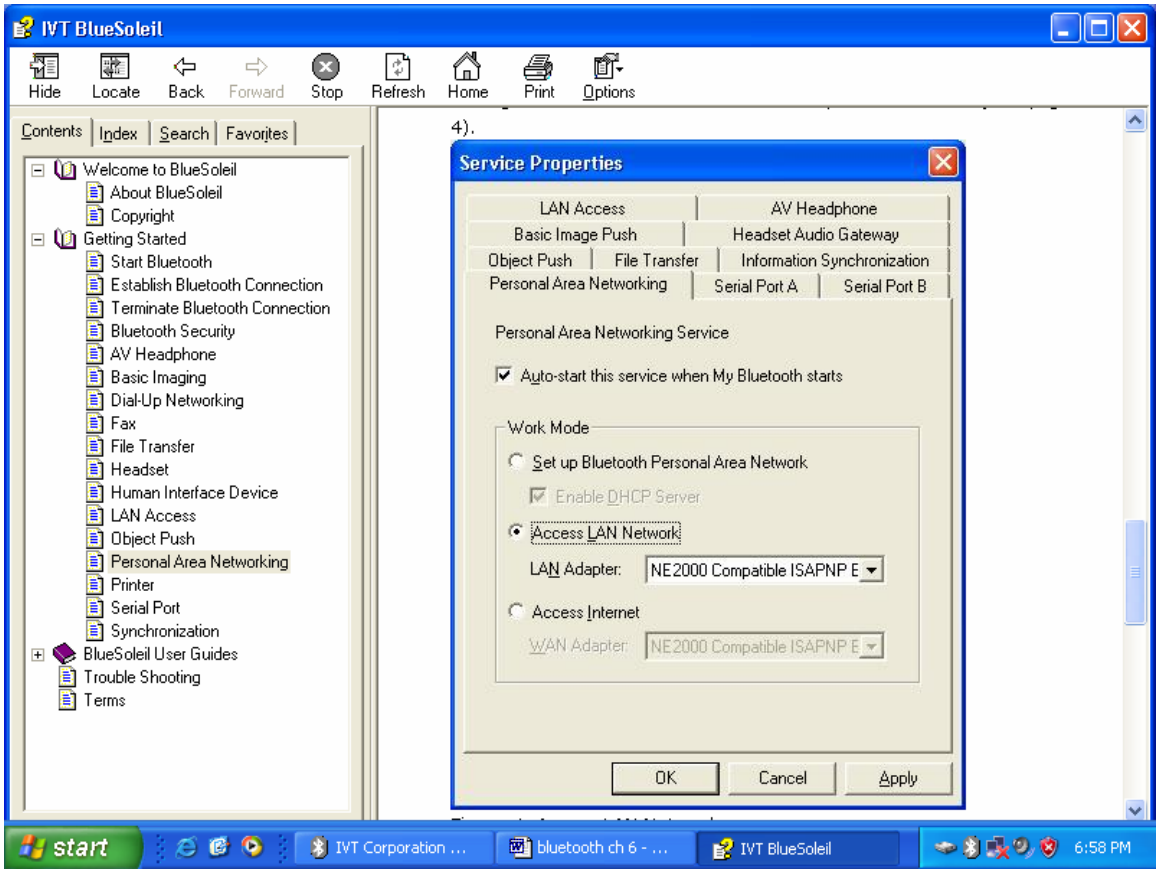


Figure 4: Access LAN Network

- **Scenario 3**: Access Internet via NAP

  Select Access Internet and select a physical network adapter, through which the NAP connects to Internet, as the WAN Adapter (Figure 5). It will automatically enables NAT (Network Address Translation, please refer to Windows Help Topic) function and a DHCP server.

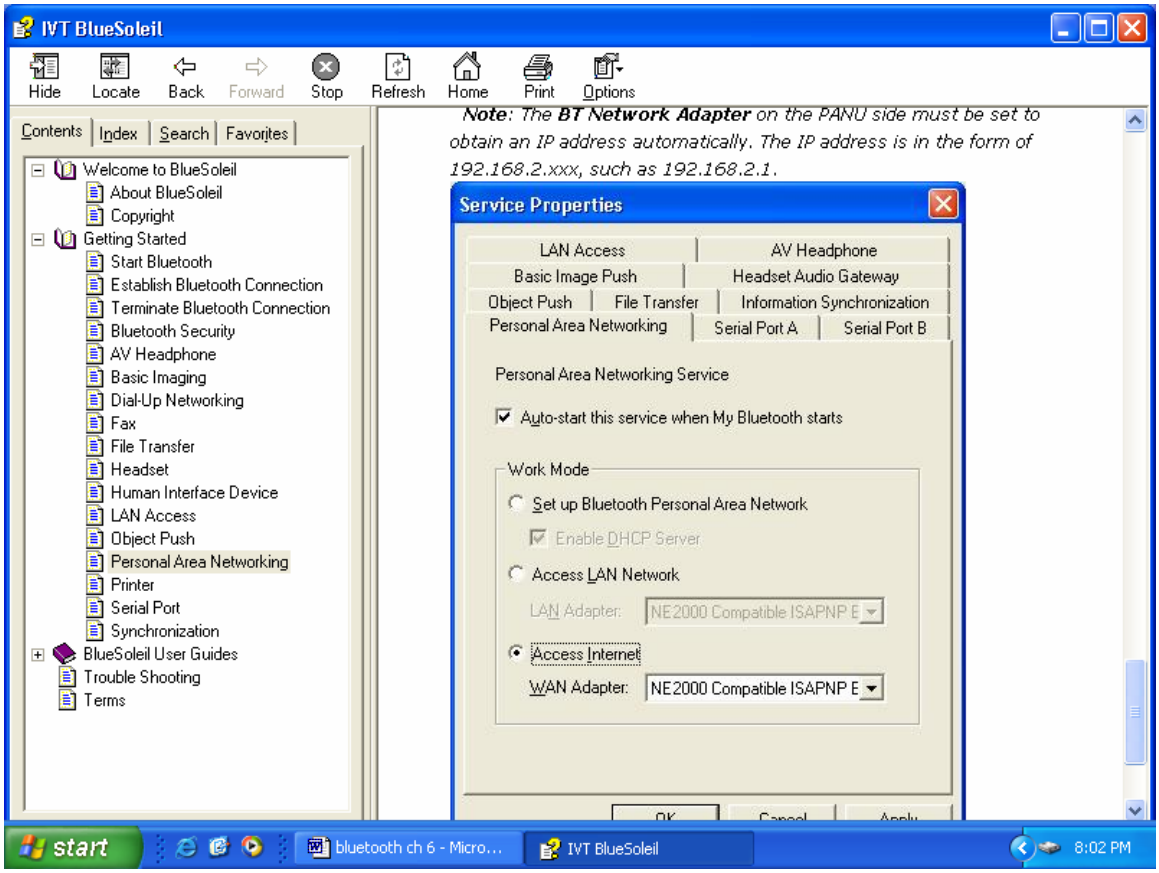


Figure 5: Access Internet

7.5.11 Printer

The Bluetooth Printer Profile (HCRP) enables your computer to connect to a Bluetooth enabled printer.

Typical Usage

- Print documents to a Bluetooth enabled Printer.

Print Documents to a Bluetooth Printer

1. Connect to the printer's printer service.
2. (a) If your computer does not have the correct printer drivers installed, BlueSoleil will prompt you to do so.

(b) If the printer driver has been installed, a message indicates the Bluetooth printer is ready.

3. Print documents using the Bluetooth enabled printer. In the application, be sure to select the correct printer and printer port.

7.5.12 Serial Port Profile

The Bluetooth Serial Port Profile (SPP) provides PCs, laptops, PDAs, GPS receivers, cordless serial adapters, and other Bluetooth enabled devices with a virtual serial port, enabling them to connect with each other wirelessly via Bluetooth instead of a serial cable.

BlueSoleil supports four Bluetooth Serial Ports for out-going connections and two Bluetooth Serial Ports for incoming connections.

Typical Usage

- Connect to other Bluetooth enabled devices via the Serial Port.

Connect to a PDA

Steps:

1. Connect the PDA's Serial Port service.
2. Use ActiveSync or any software that uses a serial connection.

7.5.13 Bluetooth Synchronization Profile

The Bluetooth Synchronization (SYNC) Profile enables users to synchronize PIM objects on their computer with that of other Bluetooth enabled computers as well as Bluetooth enabled mobile phones, PDAs, and other devices.

Four kinds of objects are supported:

- Contacts (*.vcf)
- Calendars (*.vcs)
- Notes (*.vnt)
- Messages (*.vmg)

Supported Outlook versions:

MS Outlook 2000, 2002, 2003, XP.

Typical Usage

- Synchronize your computer with a Bluetooth enabled mobile phone

7.5.13.1 Synchronize with a Bluetooth enabled Mobile Phone

Steps:

1. Connect to the mobile phone's Synchronization service.
2. A synchronization dialog will appear (refer to Figure 1). Click on the Start button to synchronize. Contacts, calendars, notes and emails in MS Outlook will be synchronized with those on the phone.

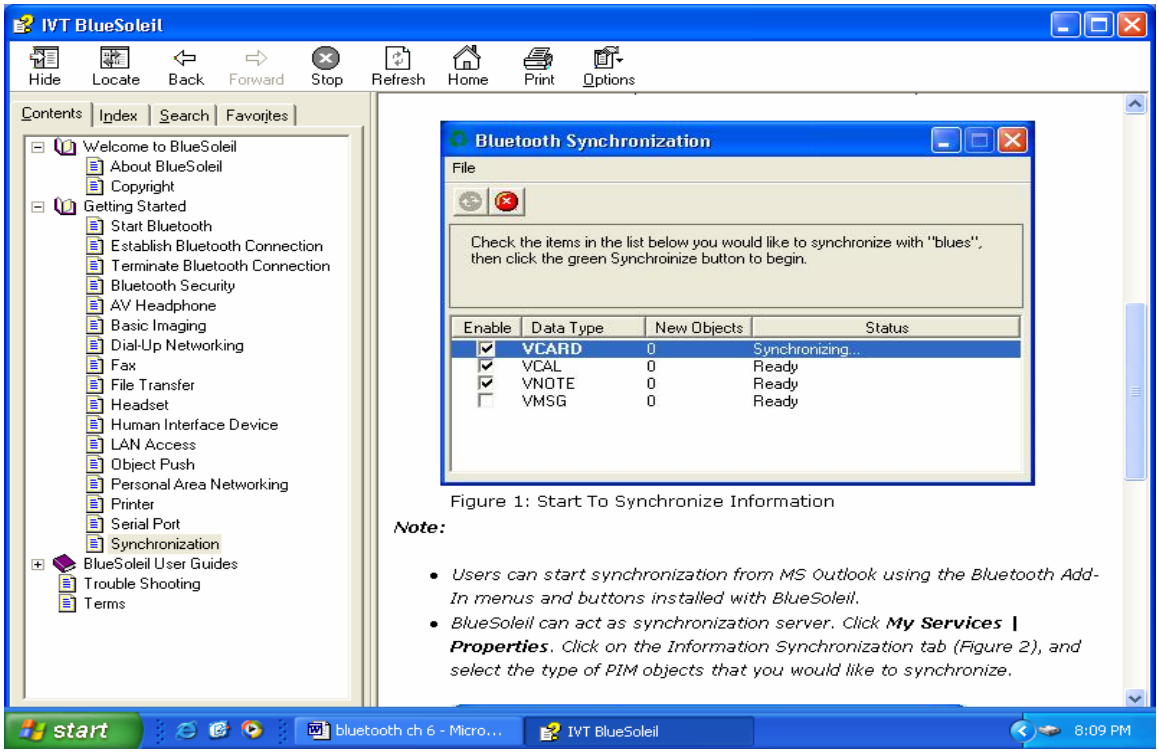


Figure 1: Start To Synchronize Information

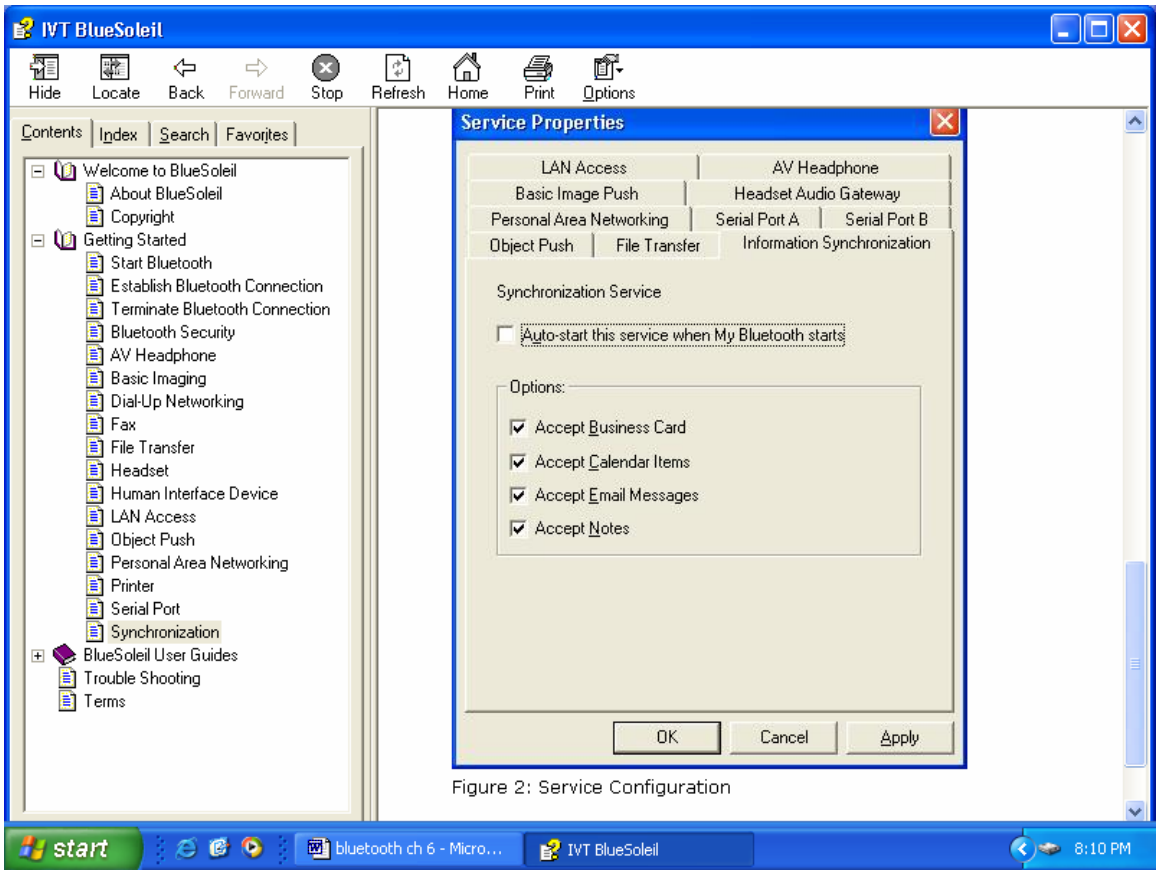


Figure 2: Service Configuration.

CHAPTER 8

IMPLEMENTATION OF BLUETOOTH PROTOCOL STACK

8.1 Hardware Selection

The next step in the design of my project was to acquire the most suitable hardware. A variety of Bluetooth hardware is available in market. Different vendors have their own hardware that is compliant to Bluetooth standards. Till now, the Bluetooth standard is not finalized and it is subject to changes. There fore the hardware available in market are compliant to a certain version of Bluetooth protocol specifications. Mainly the firmware part of hardware changes with new protocol specifications. Due to the shortage of time, I have included the main requirements concerning the selection of proper hardware:

8.2 Hardware Specs

The following issues should be considered while selecting the hardware.

8.2.1 Affordable price

The hardware should be of low cost. The hardware available in market/internet ranges from few hundred dollars to several thousand dollars.

8.2.2 Compliance to latest version of Bluetooth standard

As Bluetooth standard is still under development process we had to consider the fact that the hardware had to be compliant with latest version of specifications.

8.2.3 Interoperability with other hardware

Interoperability is the main issue. Although this was not our main requirement but a hardware that is completely compliant to Bluetooth specification, would be compatible with hardware from other manufacturers too. The advantage of this interoperability is that if we implement the protocol stack with one hardware set, it will also work with other hardware.

8.2.4 Availability of serial interface

We had to use serial interface to communicate with the hardware. The Bluetooth protocol standard provides specifications for USB as well as RS232 interface layer between the host computer and hardware.

8.2.5 Proper documentation

The hardware documentation is obviously a necessary requirement.

8.2.6 Antenna availability

Among different available hardware some have an onboard antenna; it would be preferable to get a hardware that had an onboard antenna.

8.2.7 Base band and Radio chip on same circuit

Some of the available hardware had Baseband and radio part on same board/IC, and some manufacturers provided Baseband and radio part as different Integrated Circuits. In later case we had to interface the radio IC with Baseband IC, and that was not feasible because it required extremely high precision (due to the fact that Bluetooth operates in 2.4 GHz band)

The Ericsson Bluetooth Module is a complete solution for fast implementation. It is a short-range, compact and low-cost radio/Baseband module that can be implemented in any kind of electronic device. The module includes a Baseband processor, Bluetooth radio, host and antenna interfaces and supporting circuitry, together with basic Bluetooth software for signaling at HCI (Host Control Interface) level. As the module is a generic product, it can be used for many different types of application that require a Bluetooth capability. The module supports both voice and data transmission. Communication is carried out using the module's built-in high-speed USB (Universal Serial Bus), UART or PCM interface. The module is a Power Class 2 Bluetooth device, and is qualified for Version 1.1 of the Bluetooth specification. It is also type-approved for global use including FCC/ETSI), this hardware can be ordered from http://www.comec.sigma.se. For students they have special discount, that's why we should prefer this hardware for the implementation.

8.3 Software Design

After selection of appropriate hardware, the next step is to select and/or write code for the software part.

8.3.1 Specifications

The main requirement for the software layers is, that they should be independent of each other. Any layer can be modified at any time and adopt it according to the latest specifications of Bluetooth protocol without affecting rest of the code.

8.3.2 Design Methodology

The first step in writing the software is to develop the design documents for the software layers. The design document consisted of details of each object to be used in the implementation, small description of each member of the object and small and member functions/methods of the each object. After that flow charts should be developed for each function specified in the design document.

8.4 Future Suggestions

There is enough room for improvement in this project. Following is the list of tasks that can be done.

1) **Implementation of the Protocol Stack for Point to Point Link**
2) **Extension from point to multipoint Link**
3) **Implementation of other protocols**

Other Bluetooth protocols can be implemented. These protocols are RFCOMM, SDP etc.

4) **Upgrade with new standards**

The Bluetooth is an evolving standard it specifications are subject to have further improvements in it. Although there would be no major change but minor changes are expected in the protocol standard. These changes can be easily implemented with least effort.

5) **Security**

Link level security and authentication features can be implemented.

6) **Applications**

Applications can be built on top of the protocol stack by using the API provided.

CHAPTER 9

COMPARSION WITH COMPETING TECHNOLOGIES

The following table shows a comparison between Bluetooth and other wireless communication technologies in the market.

Technology	Max. total data-rate	Range (metres)	Max. nodes	Main area of application	Cost, US$ initial/mass
IrDA (infrared)	4 Mbit/s	1 / angle 15°	2	Point-to-point data link. Peripherals: printer, keyboard	9.00 / 1.50
AIR (infrared)	4 Mbit/s	4 – 8	10	Point-to-point data link. Peripherals: printer, keyboard	9.00 / 1.50
DECT	128 kbit/s	50	8	Speech applications and point-to-point data link.	60.00 / 15.00
Bluetooth™	1 Mbit/s	10	8 (+128 inactive)	Connectivity between terminals and peripherals, cable replacement	25.00 / 3.00
HomeRF	2 Mbit/s	50	>128	Domestic data and speech networking.	30.00 / 8.00
IEEE 802.11b	11 Mbit/s	100	Around 10 per access point	Wireless LAN for data transfer including multimedia.	150.00 / 50.00
HiperLAN2	54 Mbit/s	150	Around 10 per access point	Further development of IEEE 802.11b for higher data-rates.	200.00 / 40.00

The description of the competing technologies is given below:

9.1 Infrared Technology

This standard is primarily meant for data transmission. The main differences as compared to Bluetooth are:

- IrDA is not omni directional, as is Bluetooth. The IrDA-beam has to be aimed at the receiving antenna.
- IrDA must have a free line of sight.
- IrDA is point-to-point; only 2 units at a time can communicate.
- Its maximum range is 1.5 meters with a maximum off-axis angle of 15 degree.

However, new technology from an Israeli company could find users from having to line up the infrared ports on their portables in order to exchange data. **Infra-Com** has launched infrared technology, which allows links without the communicating devices having to 'see' each other in the traditional line-of-sight way.

The line-of-sight requirement has been the force for challenging wireless technologies such as Bluetooth. But Infra-Com's new Red Beamer

technology for portable devices uses indirect and diffused infrared light, working rather like a light bulb, with light bouncing off walls and ceilings to reach the device target.

Initially, devices receiving Red Beamer will need an external infrared peripheral for data to be exchanged, but Infra-Com intends to embed the technology into devices' PCI cards. But Red Beamer's initial 56 kbps transmission speed is much slower than Bluetooth's target of 2Mbps.

After comparing the two technologies it is clear that Infrared technology has no significant future.

9.2 Area Infrared

Area Infrared (AIR) is a proposed extension to the existing IrDA standard. The beam angle is to be increased to 120 degree and the line of sight requirement eliminated. At the same time, the range is to be increased to 8 meters but the data rates will fall from 4Mbps to 250Kbps. AIR does not support speech.

9.3 DECT

DECT is the most widespread standard for digital cordless telephones and can be regarded in some respect as a forerunner of Bluetooth. With the competition from Bluetooth, it seems very unlikely that DECT will be developed any further.

9.4 Home RF

Home RF also uses 2.4GHz band, supports data rates up to 2Mbps(with plan to increase up to 10Mbps) and has a range up to 100meters. Since home RF uses two protocols, DECT for four speech channels and IEEE 802.11 for data, this technology will remain expensive than Bluetooth and also difficult to implement. Home RF and Bluetooth could co-exist.

9.5 IEEE 802.11b

IEEE 802.11 also uses the 2.4GHz band, the data rates are 11Mbps and the range is 100 meters. This standard specifies no speech transmission and its power requirements

are also high for integration into mobile phones. The cost is also high as compared to the Bluetooth.

9.6 HIPER LAN2

Some of the SIG members are developing Hiper LAN2, which should be able to work together with 3rd Generation GSM standard as a WAN and with Bluetooth as a PAN (personal Area Network). Hiper LAN2 uses 5GHz band and has a data rates up to 54Mbps with range up to 150 meters. Hiper LAN2 is suited for speech, data, multimedia content and video.

9.7 Wireless LAN

No, Bluetooth is **not** intended as a wireless extension of ordinary LANs. Both Bluetooth and WLANs are based upon the IEEE 802.11-standard. But there are too many differences for these systems to replace each other:

- WLANs are essentially ordinary LAN-protocols modulated on carrier waves. Bluetooth is more complex than that.
- Bluetooth´s essence is dynamically configured units. That's not how LANs work.
- Bluetooth hops very fast (1600 hops/second) between frequencies, which does not allow for long data blocks. A Bluetooth channel cannot handle as high data throughput as a WLAN.
- Bluetooth relies on ad-hoc-connectivity. This does not square well with (predominantly) server-based LANs.

Moreover, when a Bluetooth connection collides with a wireless LAN connection, either or both connections can jam! Bluetooth may be a boon to mobile devices, but to wireless LANs, it's a bully!!

The problem: It uses the 2.4 GHz radio frequency band, the same used by wireless LANs based on the IEEE 802.11 standard. But these two technologies have different functions. Bluetooth requires little power and is meant for transmitting small amounts of data (at 1Mbps) over short distances (up to 10 meters). 802.11 connections can range in transmission rates from 2 Mbps to 11 Mbps and at distances from 15 to about 100 meters.

9.8 Smart Cards

Well; yes and no. Contact less "smart" cards are the basis of some Bluetooth-applications. But Bluetooth goes much further than that. Smart cards:

- are point-to-point
- are not session-oriented
- have no inherent reliability when transmitting/receiving information. They are better compared with the contact less transmission-mode on the Internet.

All the functionality that”smart cards” have can be included in Bluetooth’s functionality.

9.9 Wireless Application Protocol (WAP)

”WAP - Wireless Application Protocol - is a framework specified by industry leaders supporting mobile IT-solutions”. It is a communications protocol for mobile phones, meant as an extension of available, Internet-based services. WAP only covers the higher protocol levels. There is no connection to the 802.11 standard.

CHAPTER 10

FUTURE OF BLUETOOTH TECHNOLOGY

People working within the Bluetooth industry are almost universally convinced that the future of the Bluetooth technology is bright. A large amount of market momentum has built behind concept, and support comes from both well-established firms and companies created specifically to develop new Bluetooth hardware and software. There has been some discord from the perceived competition between Bluetooth and Wi-Fi, but many recognize a market need for both. Fortunately, there doesn't yet appear to be any real challenge to Bluetooth from any other cable-replacement technology that has the potential to divide manufacturers and force costumers to select between two incompatible alternatives.

10.1 COSTUMER SATISFACTION

Clearly the most important criterion to enhance the future of Bluetooth is costumer confidence in the technology. The SIG has been focused on this aspect of Bluetooth ever since the organization was formed, and that was one of the reasons that the Bluetooth specification covers all aspects of the user interface.

The success or failure of the Bluetooth in the marketplace depends upon weather the costumer finds the technology useful, cheap, reliable, secure, and easy to operate. For Bluetooth to be *useful*, it must enable a task to be performed better than would otherwise be the case. The simple elimination of a cable is certainly useful in many applications, such as file synchronization and digital camera data transfer. However, if a set of batteries is needed to be substitute for the cable (such as mouse and keyboard), then careful power management is critically important to a successful design.

Achieving the market penetration that many manufacturers envision for Bluetooth requires it to be extremely *cheap*. Bluetooth itself is merely a communication medium, so it usually manifests itself as additional circuitry and, hence, additional cost, within a product. Many of these products are already inexpensive in their traditional manifestation, such as the remote control or headset, and costumer may balk at paying significantly paying higher prices for these items with Bluetooth compatibilities.

To be *reliable*, the Bluetooth-equipped device must have an adequate range and not be temperamental when asked to connect. Wireless devices can occasionally be troublesome (witness the mobile phones), but only rarely should this occur with

Bluetooth, and the fix should be easy, such as changing location slightly. Devices from different manufacturers should operate seamlessly.

The operation f Bluetooth-equipped devices must be *secure* and accepted as such by the costumer. Link-level security built into Bluetooth should help this situation by addressing security issues and providing consistent plateform for authentiacationand encryption across a wide range of application. As consumers become more technically literate, they begin to understand the limitations of technology as well as its benefits. Most mobile phone users are well aware of the potential for eavesdropping, and they also realize that security is important for other wireless implementations as well, including Bluetooth.

Finally, a costumer needs to find Bluetooth so *easy to operate* that it use is obvious right out of the box. The actual operation of Bluetooth is quite complex. A well designed set of controls and properly written user manual insulates the user from that complexity. This is a difficult challenge because new technology often places high demands on the consumer when it first arrives on the market.

In a nutshell, if the costumer operates a product without being aware of the Bluetooth link, then its integration can be considered a success.

10.2 Future Applications

Because Bluetooth is new, just about any application could be called futuristic, but we will take a look at a few of those that could considered an extension or addition to the Bluetooth profiles that have been published as of early 2002. Some of these are already being developed by the SIG. these applications take advantage in varying degrees of Bluetooth's capability to be always on, always connected, mobile, and easy to use. Throughout all of this, of course, it's important not to lose sight of requirement to get basic application to operate properly.

10.2.1 Local Positioning

Because the *global positioning system* (GPS) doesn't operate reliable inside buildings, Bluetooth-equipped devices could communicate with another unit that is in a

location for favorable reception of the GPS positioning information. By using a combination of RSSI, several GPS/Bluetooth nodes, and perhaps even signal arrival timing, a roaming Bluetooth-equipped device can pinpoint its location with high accuracy. This application could be extremely useful in tracking people animals as well as tracking and controlling robots and products on an assembly line.

10.2.2 Universal Remote Control

By replacing traditional IR Links with Bluetooth RF, the remote control no longer needs to be pointed at the appliance being controlled. Home theatre systems, for example, are often deployed in several locations with in the room, or even in adjacent rooms, making, Bluetooth an ideal controlling system.

10.2.3 Interactive Gaming

Connecting games via Bluetooth link gives players the ability to compete against each other rather than the computer.

10.2.4 Wireless Pen

A Bluetooth-equipped writing instrument that automatically digitizes its motion can be employed to enable the user to easily e-mail a drawing or hand written note to any receipt through an accompanying cellular phone.

10.2.5 Automotive Applications

Apart from the key less entry, Bluetooth ca be used for diagnostics, entertainment, access to other information, and navigation. Wireless communication between subsystems within the car reduces manufacturing cost by reducing the number of cable runs, connectors, fasteners, and access holes. Areas that are difficult to monitor, such as tire pressure, could be done via Bluetooth.

10.3 Operational Enhancements

What is the future for the enhancement to the basic operation of Bluetooth? Certainly, new profiles will be introduces as they are conceived, created, and approved. These will be released over time in the form of updates to the existing specification. Furthermore, sets of critical errata will be published as problems surface.

As Bluetooth matures and its capabilities and limitations are experienced in actual applications, attention will invariably turn to how its performance can be improved. Here are some of the possibilities for future enhancements to Bluetooth's operation, with emphasis on the lower protocol level.

10.3.1 Faster Data Rates

Some would argue that Bluetooth needs to increase its data rate by at least a factor of 10 to be competitive. Others argue that the present data rate is fast enough to its intended purpose. This is an area of intense debate, but its important to realize that faster data rate carries with it penalties in the form of shorter range, higher power consumption, and/or higher cost. At typical realized data rates (400 Kbps), 100 pages of printed text can be transferred in about 10 seconds and a 600 KB high-resolution digital photo in about 12 seconds. Are higher data rates worth the penalties? To answer this question, the Radio2 group has been formed within in the Bluetooth SIG to investigate higher data rates.

10.3.2 Adaptive Frequency Hoping (AFH)

AFH can reduce packet size if properly implemented. Many feel that AFH can eventually become a part of Bluetooth specification.

10.3.3 Store and Forward Capability

In its present form, Bluetooth has no formal means of increasing its range by relaying message through third parties. Of course, the feature can be implemented in higher protocols, but this can be cumbersome. Placing a store and forward capability into the specification will provide built-in commands that can be used to specify the

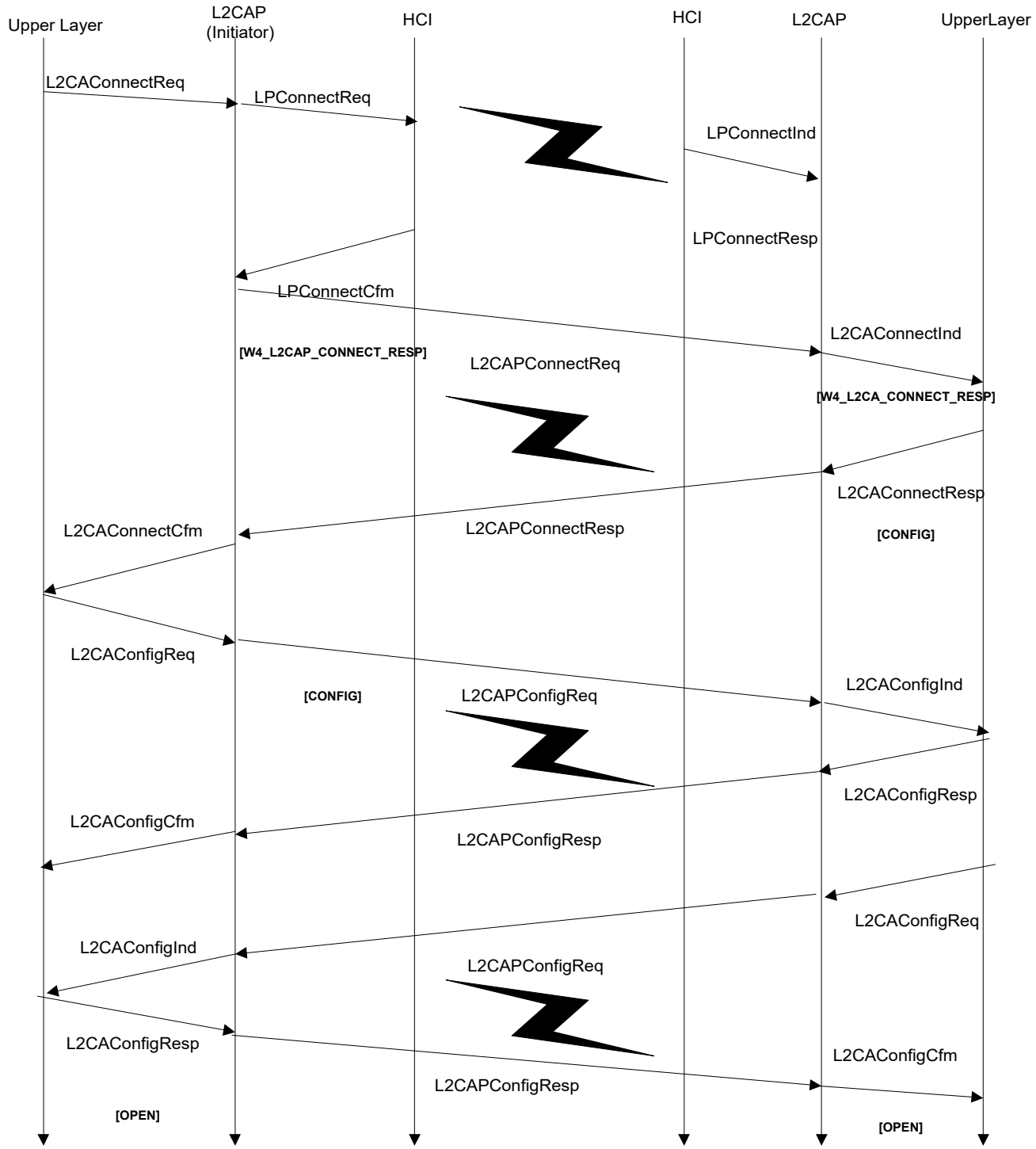
destination and, if necessary, the route that a packet should take through intermediate Bluetooth nodes. Advantages include an effected range limited only by device availability along the route and lower transmit power for closer nodes. Disadvantages include lower reliable, increased interference from multiple transmissions, reduced throughput, and higher node complexity.

10.3.4 Smart Antennas

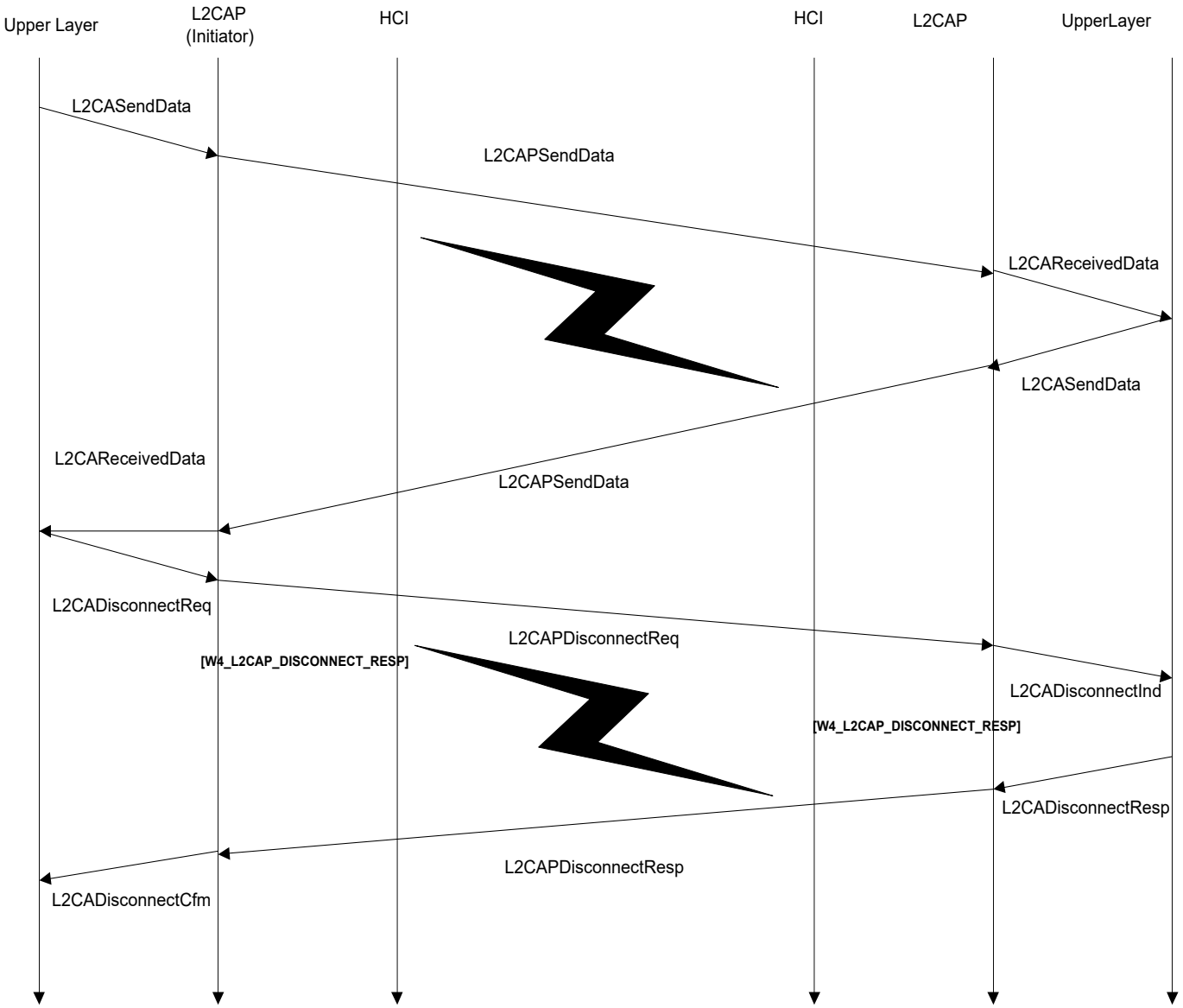
If sufficient signal processing capability is developed to control an electronically steerable antenna, then the potential exists to greatly increase performance by directing the antenna's main lobe towards the desired node. Further more, the antenna's nulls can be placed in the direction of arriving interference.

Appendix A: Message Sequence Chart

Connection Establishment and Configuration

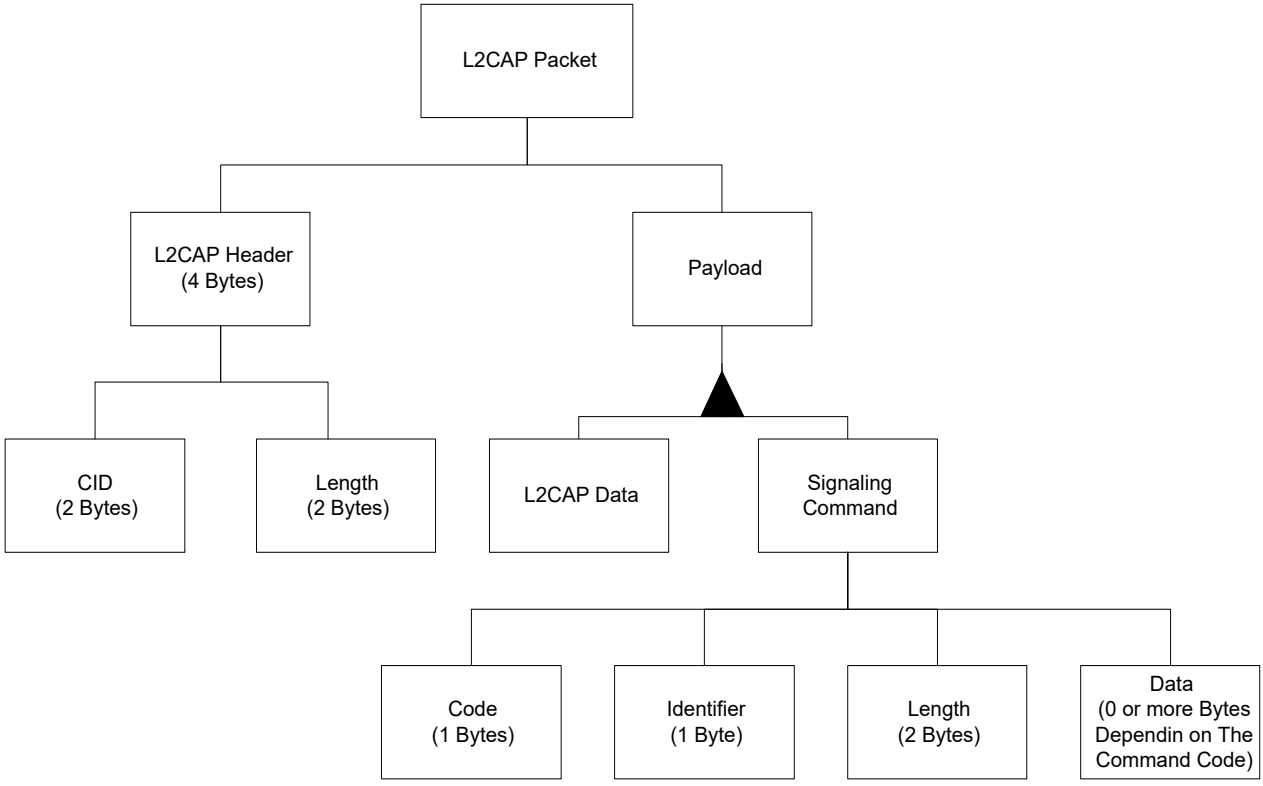


DATA TRANSMISSION AND TERMINATION OF CONNECTION



APPENDIX B: L2CAP PACKET FROMAT

L2CAP Packet Format



CONCLUSIONS AND SUGGESTIONS

CONCLUSIONS:

Bluetooth is the most widely accepted and fastest growing communications standard, which provides a universal wireless interface to a large no. of portable devices. Experts and consultants are expecting an explosive growth in Bluetooth market because of the immense requirement for low-cost and cable-free environment.

The conclusions regarding this thesis are:

- The Bluetooth technology is quite complex and in order to understand it fully one needs to have a fair knowledge of the telecommunication, electronics and data communication fields.
- The protocol stack of Bluetooth is also quite complex owing to the factor that this technology unites many devices made by different manufacturers who have their own specifications to meet with.
- This thesis may be regarded as the first step towards the implementation of the Bluetooth Protocol Stack
- The approach of " Object Oriented Programming " is a better solution for writing the applications for Bluetooth.
- Regarding hardware selection, the suggested Bluetooth modules are Ericsson's module ROK 101007 or Universal Scientific Industries 's module UB1 1112 that offer Bluetooth necessary hardware and firmware.
- Security concerns over the wireless communications are of major importance. Though these concerns are beautifully dealt in the stack yet while introducing new applications requires further security measures.
- Apart from above mentioned work, the major work is the comparison of Bluetooth with the other competing technologies. It is concluded that if our considerations are voice and data, relatively high data rates, point-to-point and point-to-multipoint connectivity, low costs and ease of using different devices, then Bluetooth is the best choice.

SUGGESTIONS:

There is ample room for improvement in this project. Following is the list of tasks that can be done.

1) Implementation of the Protocol Stack for Point to Point Link

After having at least two sets of the hardware and software, implementation of point-to-point link may be performed.

2) Extension from point to multipoint Link

Then the network may be expanded from the point-to-point link to point to multi-point links.

3) Implementation of other protocols

Other Bluetooth protocols can be implemented. These protocols are RFCOMM, SDP etc.

4) Upgrade with new standards

The Bluetooth is an evolving standard it specifications are subject to have further improvements in it. Although there would be no major change but minor changes are expected in the protocol standard. These changes can be easily implemented with least effort.

5) Security

Link level security and authentication features can be implemented.

6) Applications

Applications can be built on top of the protocol stack by using the API provided.

GLOSSARY

802.11 WLAN

A Wireless LAN specification defined by the IEEE

Access Code

Each baseband packet starts with an Access code, which can be one of 3 types, CAC, DAC & IAC. The CAC consists of a preamble, sync word and trailer, and its total length is 72 bits. When used as a self-contained message without a packet header, the DAC and IAC do not include the trailer bits and are of length 68 bits.

ACL

Asynchronous Connectionless Link. One of the two types of data links defined for the Bluetooth Systems, it is an asynchronous (packet-switched) connection between two devices created on the LMP level. This type of link is used primarily to transmit ACL packet data. The other data link type is SCO.

ACO

Authenticated Ciphering Offset.

Active Mode

In the active mode, the Bluetooth unit actively participates on the channel. The master schedules the transmission based on traffic demands to and from the different slaves. In addition, it supports regular transmissions to keep slaves synchronized to the channel. Active slaves listen in the master-to-slave slots for packets. If an active slave is not addressed, it may sleep until the next new master transmission.

AP

Access Point.

Authentication

The process of verifying 'who' is at the other end of the link. Authentication is performed for devices. In Bluetooth, this is achieved by the authentication procedure based on the stored link key or by pairing (entering a PIN).

AUX

An ACL link packet type for data. An AUX1 packet resembles a DH1 packet except it has no CRC code. As a result it can carry up to 30 info bytes.

Baseband

The baseband describes the specifications of the digital signal processing part of the hardware -- the Bluetooth link controller, which carries out the baseband protocols and other low-level link routines.

BB

Abbreviation of Baseband.

BD

Bluetooth device

BD_ADDR

Bluetooth Device Address. Each Bluetooth transceiver is allocated a unique 48-bit device address. It is divided into a 24-bit LAP field, a 16-bit NAP field and an 8-bit UAP field.

BER

Bit Error Rate

Bluetooth

An open specification for wireless communication of data and voice. It is based on a low-cost short-range radio link facilitating protected ad hoc connections for stationary and mobile communication environments.

Bluetooth clock

Every Bluetooth unit has an internal system clock, which determines the timing and hopping of the transceiver. It is never adjusted or turned off. It can be implemented as a 28-bit counter, with the LSB ticking in units of 312.5us, giving a clock rate of 3.2kHz.

Bluetooth device class

A parameter that indicates the type of device and which types of services that are supported. The class is received during the discovery procedure.

Channel

A logical connection on the L2CAP level between two devices serving a single application or higher layer protocol.

Channel (hopping) sequence

This is a pseudo-random sequence of 79 (23 for the 23MHz system) frequencies; the frequency is calculated using the BD_ADDR of the master of the piconet. The phase in the sequence is derived from an estimate of the master's clock. The channel hopping sequence has a very long period length, does not show repetitive patterns over a short time interval, but which distributes the hop frequencies equally over the 79 (23 for the 23MHz system) MHz during a short time interval .See also Frequency sequence.

Circuit Switched Bluetooth

The application of a network where a dedicated line is used to transmit Bluetooth data.

CL

Connectionless.

CLK

Clock, typically the master device clock which defines the timing, used in the piconet.

CO

Connection-oriented.

CoD

Class of Device.

Connectable device

A Bluetooth device in range that will respond to a page message and set up a connection

CRC

Cyclic Redundancy Check. This is a 16-bit code added to the packet to determine whether the payload is correct or not. CRC data payloads can be carried only be DM, DH or DV packets. The CRC code is generated by the CRC-CCITT polynomial 0x11021 (hex).

CVSD

Continuous Variable Slope Delta Modulation.

DCID

Destination Channel Identifier, used as the device local end point for an L2CAP transmission. It represents the channel endpoint on the device receiving the message. It is a device local name only. See also SCID.

Destination

The Bluetooth device receiving an action from another Bluetooth device. The device sending the action is called the source. The destination is typically part of an established link, though not always (such as in inquiry / page procedures).

FEC

Forward Error Correction. The purpose of the FEC scheme on the data payload is to reduce the number of retransmissions. Within Bluetooth, there are 2 versions of this, 1/3 FEC and 2/3 FEC. 1/3 FEC is a simple 3-times repetition of each info bit. 2/3 FEC is a (15,10) shortened Hamming code.

FH

Frequency Hopping.

FHS

Frequency Hopping Synchronization. This a special control packet revealing, among other things, the BD_ADDR and the clock of the source device. It contains 144 info bits and a 16-bit CRC code. The payload is coded with a rate 2/3 FEC that brings the total payload length to 240 bits. The FHS packet covers a single time slot. See also Bluetooth packet types.

GAP

Generic Access Profile. This profile describes the mechanism by which one device discovers and accesses another device when they do not share a common application.

GFSK

Gaussian Frequency Shift Keying. This is the modulation used in the radio layer of the Bluetooth system.

HCI

Host Controller Interface. An (application-optional) layer, which provides a command interface to the LMP and Baseband layers.

Hold mode

Devices synchronized to a piconet can enter power-saving modes in which device activity is lowered. The master unit can put slave units into HOLD mode, where only an internal timer is running. Slave units can also demand to be put into HOLD mode. Data transfer restarts instantly when units transition out of HOLD mode. It has an intermediate duty cycle (medium power efficient) of the 3 power saving modes (sniff, hold & park).

Inquiry Procedure

The inquiry procedure enables a device to discover which devices are in range, and determine the addresses and clocks for the devices. The inquiry procedure involves a unit (the source) sending out inquiry packets (**inquiry** state) and then receiving the inquiry reply. The unit that receives the inquiry packets (the destination) will hopefully be in the **inquiry scan** state to receive the inquiry packets. The destination will then enter the **inquiry response** state and send an inquiry reply to the source. After the inquiry procedure has completed, a connection can be established using the paging procedure.

ISM

Industrial Scientific Medical.

L2CAP

Logical Link Controller and Adaptation Protocol. This protocol supports higher-level protocol multiplexing, packet segmentation and reassembly, and the conveying of quality of service information.

L_CH

Logical Channel.

LAP

LAN Access Point.

LC

Link Controller. The Link Controller manages the link to the other Bluetooth devices. It is the low-level baseband protocol handler.

LM

Link Manager. The Link Manager software entity carries out link setup, authentication, link configuration, and other protocols.

LMP

Link Manager Protocol. The LMP is used for link setup and control. The LMP PDU signals are interpreted and filtered out by the Link Manager on the receiving side and are not propagated to higher layers.

Logical Channel

There are 5 logical channels defined for the Bluetooth system. The LC & LM control channels, and the UA, UI & US user channels. The LC channel is carried in the packet header, all other channels are carried in the packet payload. See the individual sections for more details.

MAC Address

3-bit address to distinguish between units participating in the piconet. Within Bluetooth, this is the AM_ADDR .

Master device

A device that initiates an action or requests a service on a piconet. Also the device in a piconet whose clock and hopping sequence are used to synchronize all other devices in the piconet. See also LocDev.

MSC

Message Sequence Chart.

Packet Header

The header contains link control info and consists of 6 fields: AM_ADDR: active member address, TYPE: type code, FLOW: flow control, ARQN: acknowledge indication, SEQN: sequence number & HEC: header error check. The total size of the header is 54-bits.

Packet Switched

A network that routes data packets based on an address contained in the data packet is said to be a packet switched network. Multiple data packets can share the same network resources.

Packet type

13 different packet types are defined for the baseband layer of the Bluetooth system. All higher layers use these packets to compose higher-level PDUs. The packets are ID, NULL, POLL, FHS, DM1; these packets are defined for both SCO and ACL links. DH1, AUX1, DM3, DH3, DM5, DH5 are defined for ACL links only. HV1, HV2, HV3, DV are defined for SCO links only.

Page Scan State

A mode where a device listens for page trains containing its own device access code (DAC). When a device wishes to receive page packets it enters the page scan mode. The scanning will follow the page hopping sequence. If a device receives a page packet, it will enter the slave response state.

Page State

A mode that a device enters when searching for other devices. The device sends out a page packet (ID packet), using the page hopping sequence, to notify other devices that it wants to know about the other devices and/or their services.

Paging Procedure

With the paging procedure, an actual connection can be established. The paging procedure typically follows the inquiry procedure. Only the Bluetooth device address is required to set up a connection. Knowledge about the clock (clock estimate) will accelerate the setup procedure. A unit that establishes a connection will carry out a page procedure and will automatically be the master of the connection. The procedure occurs as follows:

1: A device (the source) pages another device (the destination): **Page** state

2: The destination receives the page: **Page Scan** state

3: The destination sends a reply to the source. : **Slave Response** state: Step 1

4: The source sends an FHS packet to the destination: **Master Response** state: Step 1

5: The destination sends it's second reply to the source. : **Slave Response** state: Step 2

6: The destination & source then switch to the source channel parameters: Master **Response** state: Step 2 **&** Slave **Response** state: Step 3

Park mode

In the PARK mode, a device is still synchronized to the piconet but does not participate in the traffic. Parked devices have given up their MAC (AM_ADDR) address and occasional listen to the traffic of the master to re-synchronize and check on broadcast messages. It has the lowest duty cycle (power efficiency) of all 3 power saving modes (sniff, hold & park).

Payload format

Each packet payload can have one of 2 possible fields, the data field (ACL) or the voice field (SCO). The different packets, depending on whether they are ACL or SCO packets can only have one of these fields. The one exception is the DV packets, which have both. The voice field has a fixed length field, with no

payload header. The data field consists of 3 segments: a payload header, a payload body and a CRC code (with the exception of the AUX1 packet).

PDU

Protocol Data Unit. (i.e. a message.)

Physical link

A synchronized Bluetooth baseband-compliant RF hopping sequence. It is a baseband level association between two devices established using paging. A physical link comprises a sequence of transmission slots on a physical channel alternating between master and slave transmission slots.

Piconet

A collection of devices connected via Bluetooth technology in an ad hoc fashion. A piconet starts with two connected devices, such as a portable PC and cellular phone, and may grow to eight connected devices. All Bluetooth devices are peer units and have identical implementations. However, when establishing a piconet, one unit will act as a master and the other(s) as slave(s) for the duration of the piconet connection. All devices have the same physical channel defined by the master device parameters (clock and BD_ADDR).

Profile

A description of the operation of a device or application.

QoS

Quality of Service.

Radio

The Radio layer of the Bluetooth system, the lowest defined layer. It details the requirements needed for a Bluetooth device transceiver to operate in the Bluetooth radio band. 2 different ranges have been defined for the radio layer, a 23MHz range and a 79MHz range, both are in the 2.4GHz ISM band. The 23MHz

range is only used in certain countries (such as Spain, France) that have national limitations on the amount of frequencies available. Different hop systems are used for both.

RFCOMM

Serial Cable Emulation Protocol based on ETSI TS 07.10.

RS-232

A serial communications interface. Serial communication standards are defined by the Electronic Industries Association (EIA).

RTX Timer

The Response Timeout eXpired timer used in the L2CAP layer to terminate the channel when the remote endpoint is unresponsive to signaling requests. It is started when a signaling request is sent to a remote device.

SAP

Service Access Points.

SAR

Segmentation and Reassembly. A sub layer of the L2CAP layer.

Scatternet

Multiple independent and non-synchronized piconets form a scatternet.

SCO

Synchronous Connection Oriented link. One of the 2 Bluetooth data link types defined. A synchronous (circuit-switched) connection for reserved bandwidth communications, e.g. voice, between two devices created on the LMP level by reserving slots periodically on a physical channel. This type of link is used primarily to transport SCO packets (voice data). SCO packets do not include a CRC and are never retransmitted. It primarily supports time-bounded information

like voice. (Master to single slave.) SCO links can be established only after an ACL link has first been established. See also ACL.

SCID

Source Channel Identifier. Used in the L2CAP layer to indicate the channel endpoint on the device sending the L2CAP message. It is a device local name only. See also DCID.

SDP

Service Discovery Protocol. It is a Bluetooth defined protocol for provided for or available through a Bluetooth device. Essentially provides a means for applications to discover which services are available and to determine the characteristics of those available services.

Service Attribute

Each service attribute describes a single characteristic of a service.

Service Discovery

See SDP.

SIG

Special Interest Group. The Bluetooth SIG is located at www.bluetooth.com.

Slave device

A device in a piconet other than the master. There can be many slaves per piconet.

Sniff mode

Devices synchronized to a piconet can enter power-saving modes in which device activity is lowered. In the SNIFF mode, a slave device listens to the piconet at reduced rate, thus reducing its duty cycle. The SNIFF interval is programmable

and depends on the application. It has the highest duty cycle (least power efficient) of all 3 power saving modes (sniff, hold & park).

Source

The Bluetooth device, which initiates an action with another Bluetooth device. The device receiving the action is called the destination. The source is typically part of an established link, though not always (such as in inquiry / page procedures).

SR

Scan Repetition. A mode used in the baseband layer to determine how long the device will continue to scan for a page response

Time slot

A single time slot in the Bluetooth system lasts 625us. It can be though of as the time it takes to send one packet from one Bluetooth device to another

WLAN

Wireless Local Area Network.

REFERENCES

[1] ***Bluetooth Implementation and Use*** *"**Robert Marrow**" Mc. Graw Hill Professionals, May 2002.*

[2] ***Wireless Communication Principles and Practice " Theodore S. Rappaport"*** *Prentice Hall, 2nd Edition, 2002.*

[3] ***Discovering Bluetooth "Michael Miller"*** *Cyber Incorporated, July 2001.*

[4] ***Wireless Communication Technology "Roy Blake"*** *Delmar Thomas Learning, 2001.*

[5] ***Residential Broadband*** *" George Abe" Cisco Press, 2000.*

[6] ***Bluetooth Revealed "Brent A. Miller" Prentice Hall, September 2000***

[7] ***Bluetooth Demystified*** *"**Nathan J. Miller**" Mc. Graw Hill Professionals, September 2000.*

[8] **www.bluetooth.com**

[9] **www.bluetooth.ericsson.com**

[10] **www.infotooth.com**

[11] **www.itpapers.com**

[12] **www.bluelink.com**

[13] **www.rfi.de**

[14] **www.usi.com**

[15] **www.enea.com**

[16] **www.pcibm.com**

[17] **www.intel.com**

[18] **www.lucent.com**

[19] **www.nokia.com**

[20] **www.siliconwave.com**

[21] **www.toshiba-europe.com**

[22] **www.socketcom.com**

[23] **www.motorola.com**

[24] **www.3com.dk**

[25] **www.teledotcom.com**